پروتکلهای توزیع کلید دوسویه

Two-Parti Key Distribution Protocols

فهرست مطالب

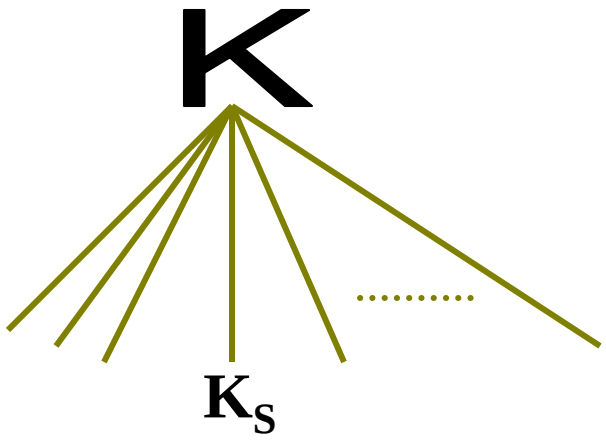
- اصول پروتکلهای توزیع کلید
- پروتکلهای توزیع کلیدغیرمتمرکز مبتنی بر رمز متقارن
- پروتکلهای توزیع کلیدغیرمتمرکز مبتنی بر رمز نامتقارن
- پروتکلهای توزیع کلید متمرکز مبتنی بر رمز متقارن
- جمع بندی

اصول پروتکلهای

توزیع کلید

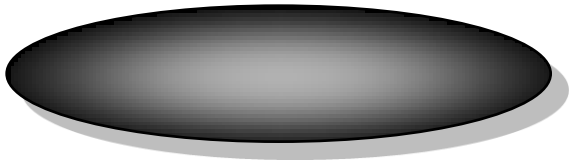
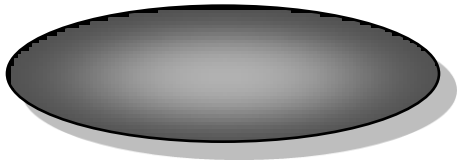
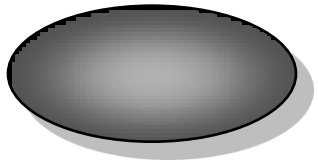
اصول پروتکلهای توزیع کلید

کلید و سلسله مراتب آن



- کلید اصلی (برای رمز کلیدها)
- کلید جلسه (برای رمز داده ها)

سلسله مراتب کلیدها

نحوه محافظت	حجم اطلاعات	نوع
محافظت با رمزنگاری		داده
محافظت با رمزنگاری		کلید جلسه
محافظت فیزیکی		کلید اصلی

کلید جلسه و کلید اصلی: مقایسه

- کلید اصلی:
  - طول عمر نسبتاً زیاد،
  - میزان استفاده محدود(فقط رمز نگاری کلیدهای جلسه)،
  - خسارت گسترده درصورت افشاء
- کلید جلسه:
  - طول عمر نسبتاً کوتاه،
  - استفاده نامحدود در طول جلسه،
  - خسارت محدود به داده های جلسه

طول عمر کلید جلسه

یک مصالحه میان *امنیت* و *کارایی* بر سر تعیین طول عمر کلید جلسه بر قرار است.

- طول عمر کوتاه:
  - امنیت بالا
    - حجم داده برای تحلیل رمز ناچیز است
    - میزان استفاده کم است
    - حتی پس از افشای کلید، زمان زیادی برای سوء استفاده موجود نیست.
  - کارایی کم
    - دائما باید کلید را به روز کنیم
- طول عمر زیاد:
  - کارایی بالا، امنیت کم

مبانی پروتکل های برقراری کلید

- پروتکل:
  - یک فرآیند چند سویه متشکل از زنجیره‌ای از قدمهاست که بایستی به دقت از سوی دو یا چند طرف برای دستیابی به یک هدف معین اجرا گردد.
  - مجموعه قواعدی که بین دو یا چند عامل در شبکه به منظور تبادل اطلاعات قرار داد می‌شود.
  - هرگاه که **هدف** از اجرای پروتکل دستیابی به یک **مؤلفه امنیتی** باشد، آنرا **پروتکل امنیتی** می‌نامند.
    - پروتکلهای امضا، پروتکلهای احراز اصالت و ... .

تعریف پروتکل های برقراری کلید

برقراری کلید مشترک به طور امن بین طرفهای پروتکل

جنبه های مختلف امنیت در برقراری کلید:

- پنهان سازی (secrecy)
- درستی (integrity)
- احراز اصالت طرفها (entity authentication)

انکارناپذیری (non-repudiability)

قابلیت دسترسی (availability)

فهرست حملات

- حمله تکرار (replay attack):
  - با تکرار غیر مجاز پیامهای مجاز نسخه برداری شده
  - آسیب پذیری به علت عدم احراز تازگی پیام
- حمله انعکاس(reflection attack)
  - دشمن پیام اخذ شده را مجددا برای مبداء می فرستد تا با بهره گیری از پاسخ آن، پاسخ پیام اول را ارائه نماید (ایجاد جلسه موازی با جلسه اول)
- حمله درهمبافی (interleaving attack)
  - دشمن با برقراری چند جلسه موازی به طور همزمان نقشهای مختلفی را ایفا می کند. دشمن پیام دریافتی از یک طرف را برای طرف دیگر ارسال می کند تا از پاسخ آن، پاسخ پیام اول را ارائه کند.

فهرست حملات

- حمله نوع (type attack)

در صورتی که فرمت پیامها یا بخشهایی از آنها با هم سازگار باشند دشمن قادر خواهد بود آنها را به جای یکدیگر مورد استفاده قرار دهد.

- حمله کلید معلوم (known key attack)

دشمن با فرض در اختیار داشتن کلیدهای قبلی به دنبال استنتاج کلید جلسه فعلی است.

- حملات وابسته به پیاده سازی
- حملات وابسته به سیستم رمز

اهداف امنیتی

امنیت و کلید:

- پنهان سازی : کلید باید از چشم دشمن مخفی باشد. اجرای پروتکل نباید هیچ ایده ای بهتر از حدس تصادفی کلید در اختیار دشمن بگذارد.

Perfect Forward Secrecy: اگر دشمن داده های رمز شده را ذخیره کرده باشد و پس از آن موفق به کشف کلید اصلی و یا **long term** شود، نتواند داده ها را رمز گشایی کند.؟!؟!

- درستی
- تازگی

عوامل مؤثر در کارآمدی

- میزان پردازش مقدماتی
- میزان نیاز به طرف سوم
- تعداد پیامها (تاخیر)
- پهنای باند مورد نیاز (طول پیامها)
- حجم محاسبات
- نیازبه همزمانی طرفها
- نیاز به حفظ وضعیتها
- امکان ارتباط متعاقب ساده شده

ابزارهای ارزیابی پروتکلها

- رویکرد شهودی (Heuristic Methods)
  - امنیت عملی
- روشهای شکلی(Formal Methods)
  - اثبات درستی
  - بازسازی حمله
- روشهای غیرشکلی(Informal Methods)
  - امنیت قابل اثبات

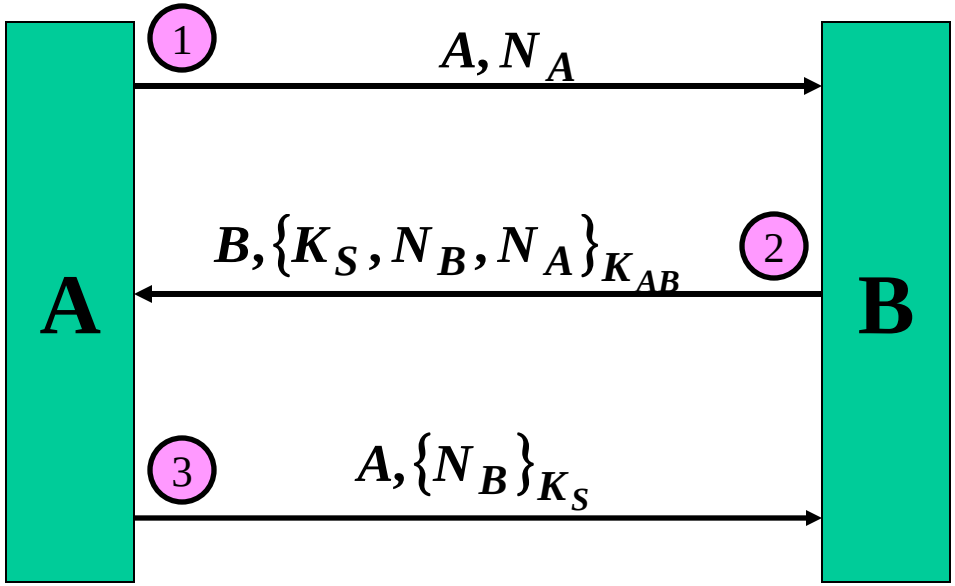
Concepts and Classification

- Key establishment: a shared secret becomes available to two or more parties, for subsequent cryptographic use.
  - key transport protocol
    - one party creates, and securely transfers it to the other(s).
  - key agreement protocol: key establishment technique in which
    - a shared secret is derived by two (or more) parties
  - key pre-distribution vs. dynamic(session) key establishment

- Use of trusted servers
  - trusted third party, trusted server, authentication server, key distribution center (KDC), key translation center (KTC) and certification authority (CA).

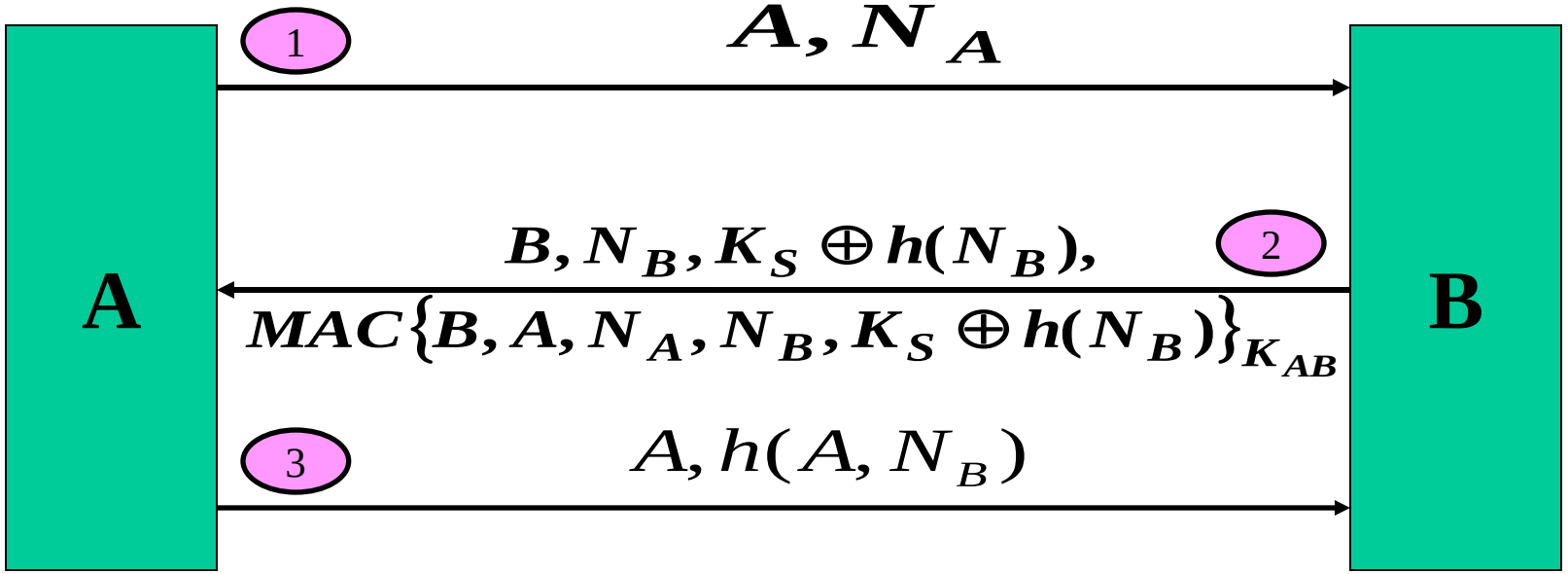
پروتکلهای غیرمتمرکز مبتنی بر رمزمتقارن

پروتکل پایه



پارامتر	نماد گذاری
نانس	N_X
کلیداصلی	K_{XY}
کلیدجلسه	K_S
شناسه آغازگر	A
شناسه مخاطب	B
عبارت رمز شده (دوطرفه)	$\{\}_{K_{XC}}$
عبارت رمز شده (یک طرفه)	$MAC\{\}_{K_{XC}}$
مبادله پیام بین طرفها	$X \rightarrow Y : ....$

پروتکل AKEP1



$$h(N_B) = MAC\{N_B\}_{K_{AB}}$$

مزیت:

عدم استفاده از رمزدوطرفه

پروتکلهای توزیع کلیدغیرمتمرکز مبتنی بر رمز متقارن

- نیاز به توافق بر روی کلید پیش از برقراری ارتباط بین هر دو نفر
- عدم مقیاس پذیری:
  - برای ارتباط n نفر باهم به $n(n-1)/2$ کلید احتیاج داریم.

دو رویکرد اساسی برای رفع اشکال

- پروتکلهای غیرمتمرکز مبتنی بر رمز نامتقارن
- پروتکلهای متمرکز مبتنی بر رمز متقارن

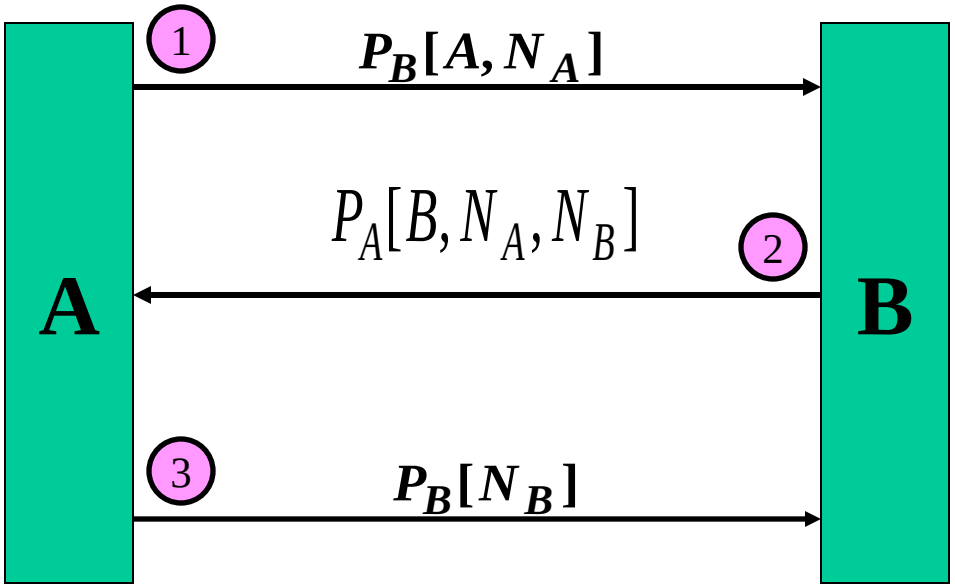
رویکرد اول (متداول)

- استفاده از سیستم رمز کلید عمومی
  - بکارگیری مکانیزم رمز (P)
  - بکارگیری مکانیزم امضا (S)
  - بکارگیری توام مکانیزمهای رمز و امضا (P و S)

بکارگیری مکانیزم رمز (P)

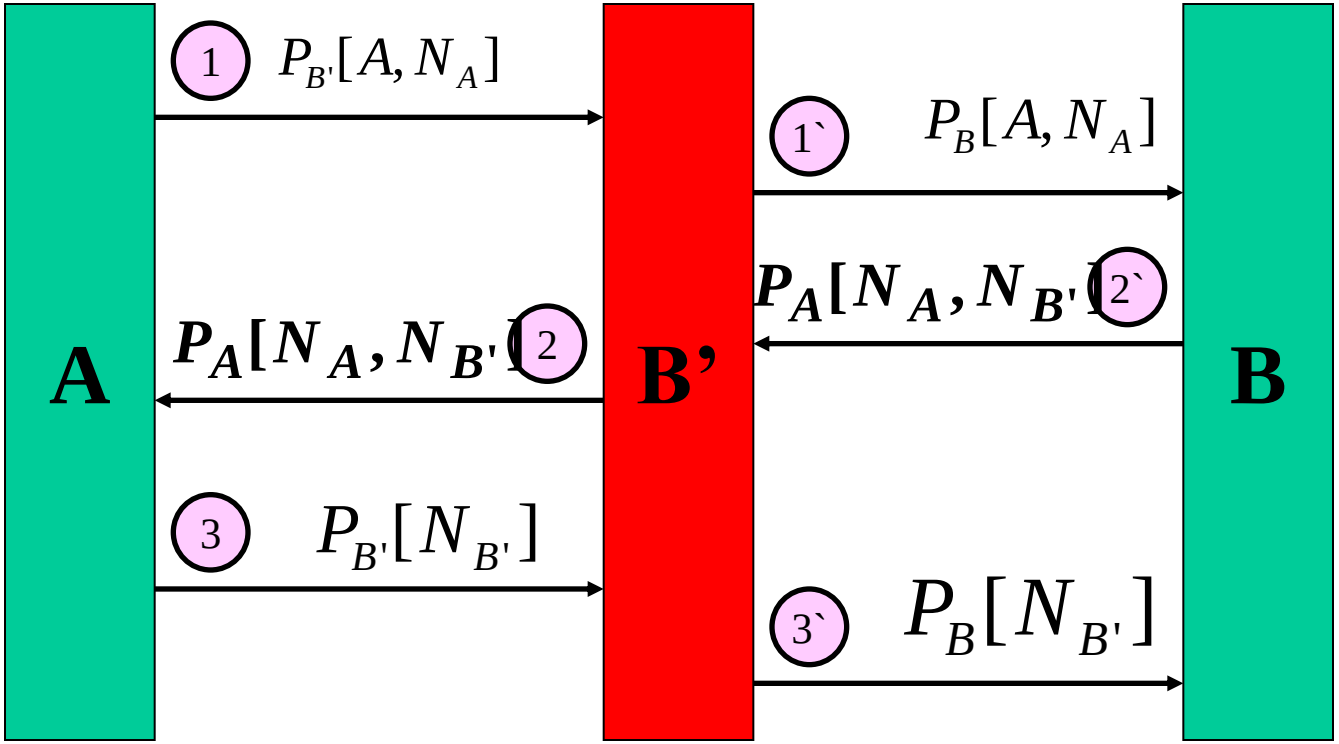
$$D_d(E_e(\mathrm{M})) = \mathrm{M}$$

- مثال: پروتکل **Needham-Schroeder**

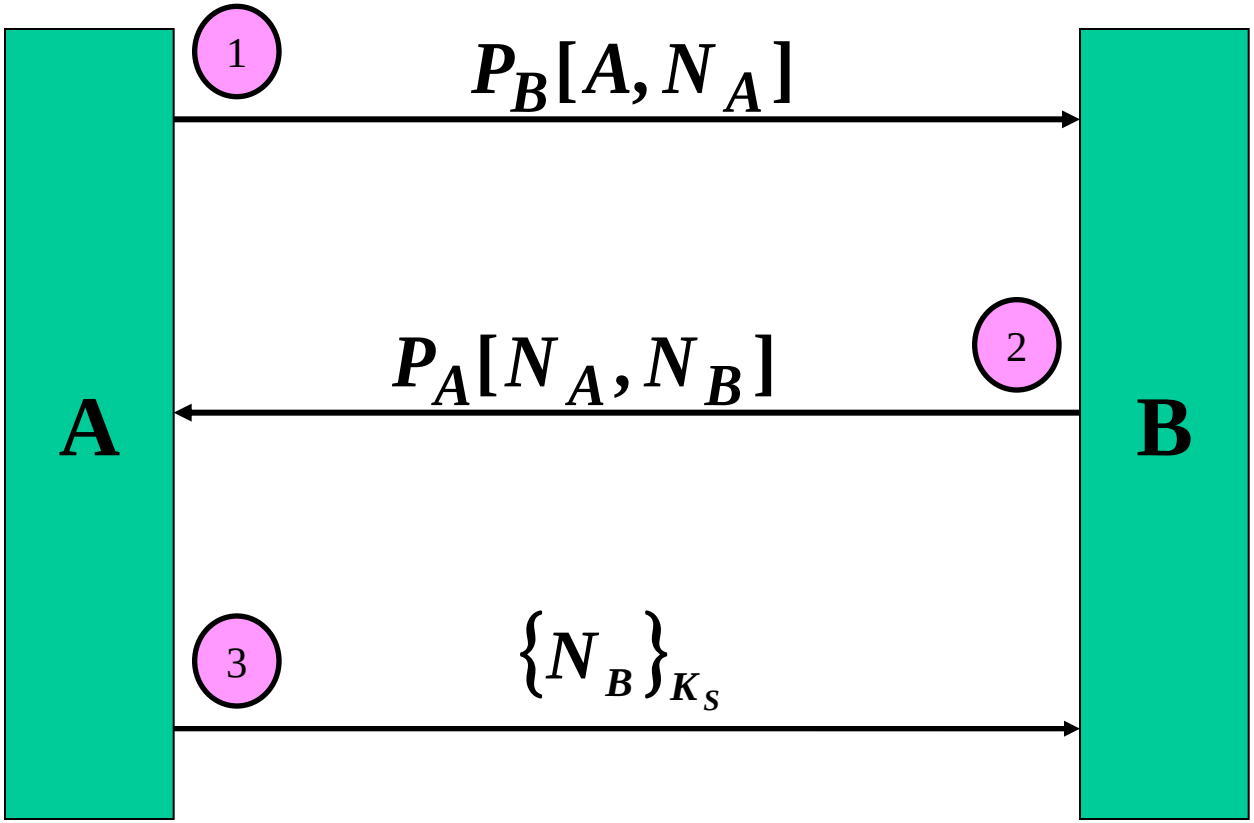


$$K_s = H(N_A \| N_B)$$

فرایند حمله



اصلاحیه ۱: پروتکل Needham-Schroeder



پروتکلهای متمرکز
مبتنی بر رمز متقارن

انواع الگوهای ارتباطی

- **PUSH** :

  تنها آغازگر بطور مستقیم با مرکز در ارتباط است

- **PULL** :

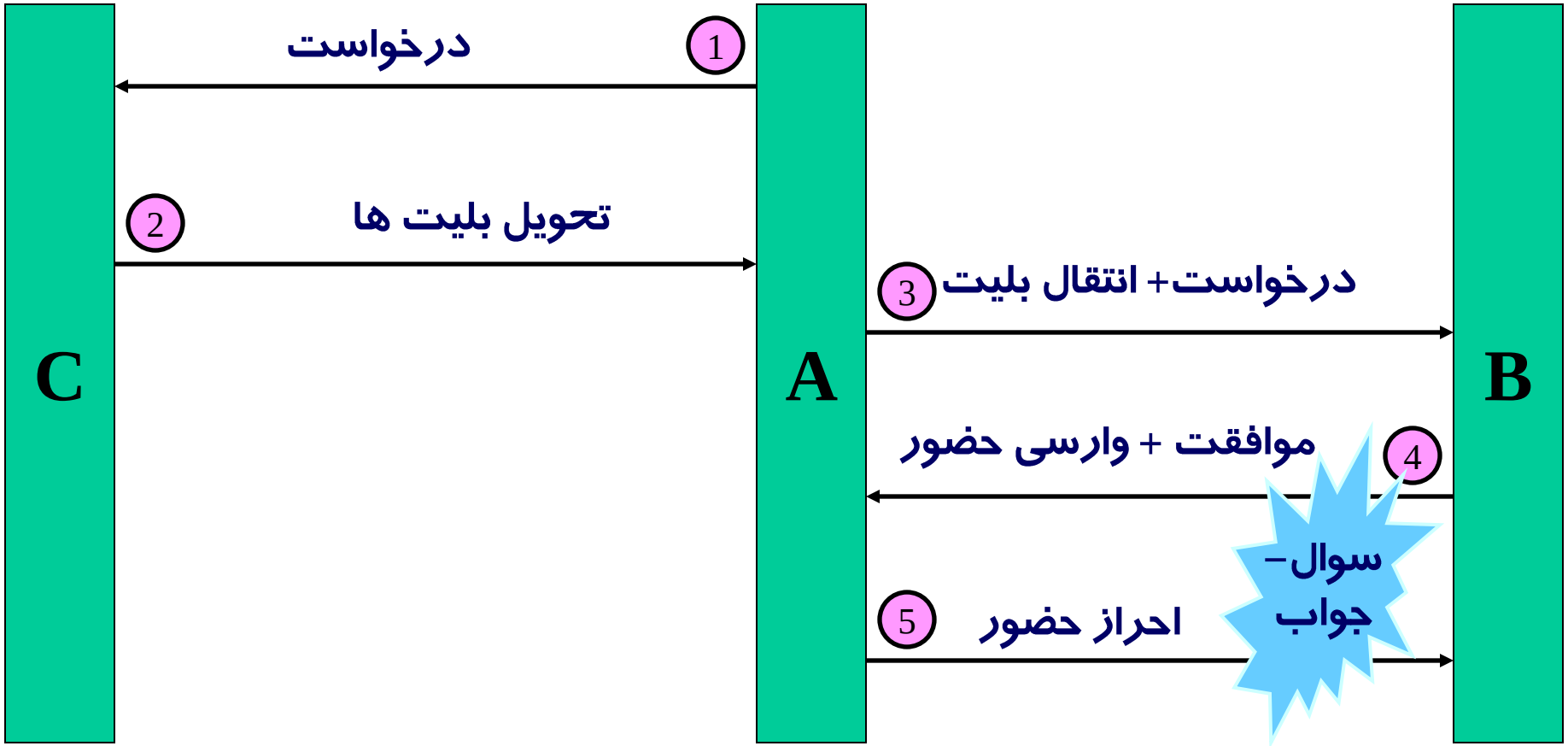
  تنها مخاطب بطور مستقیم با مرکز در ارتباط است

- مخلوط (**MIXED**) :

  هر دو طرف بطور مستقیم با مرکز در ارتباط هستند

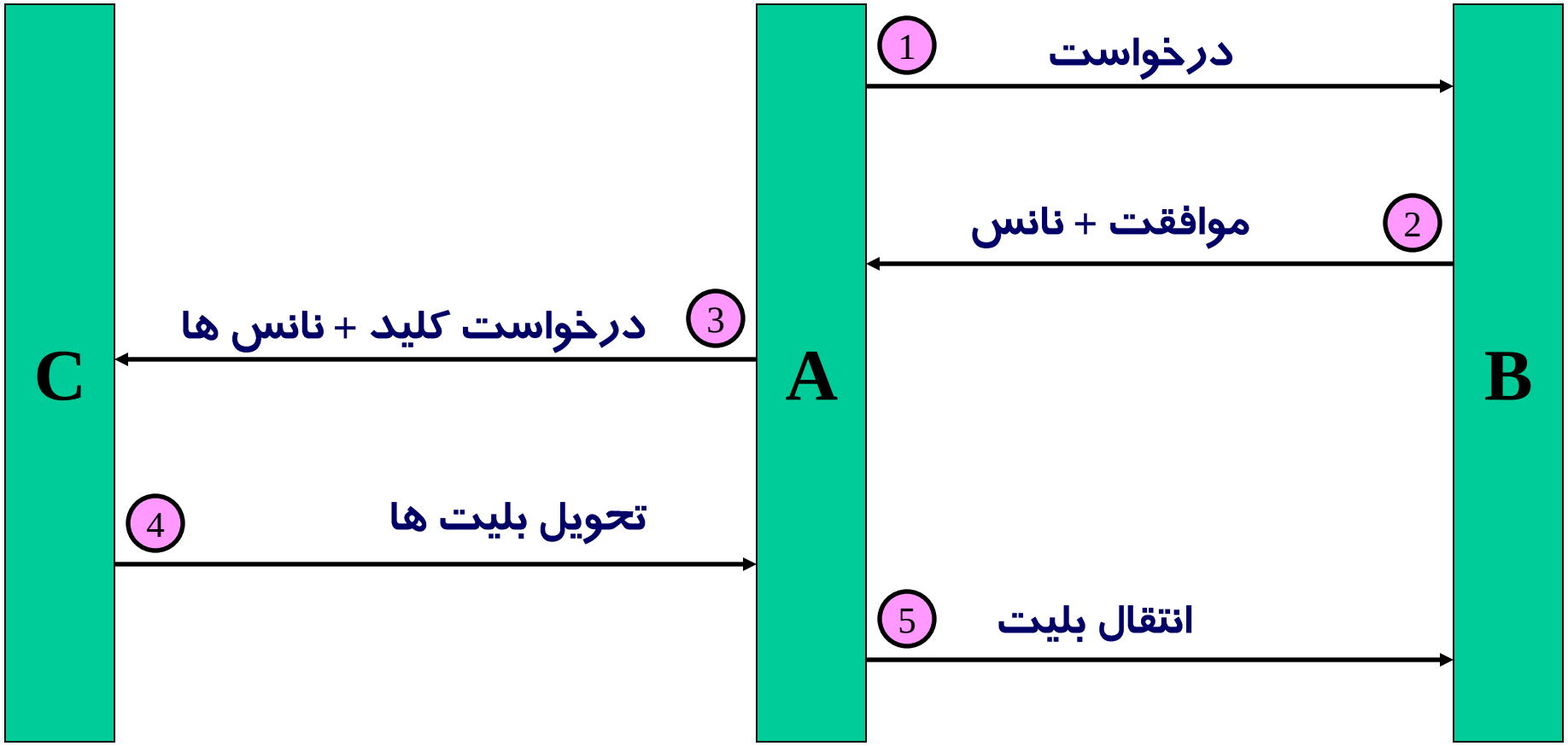
پروتکلهای مبتنی بر الگوی PUSH

سناریوی ۱ :



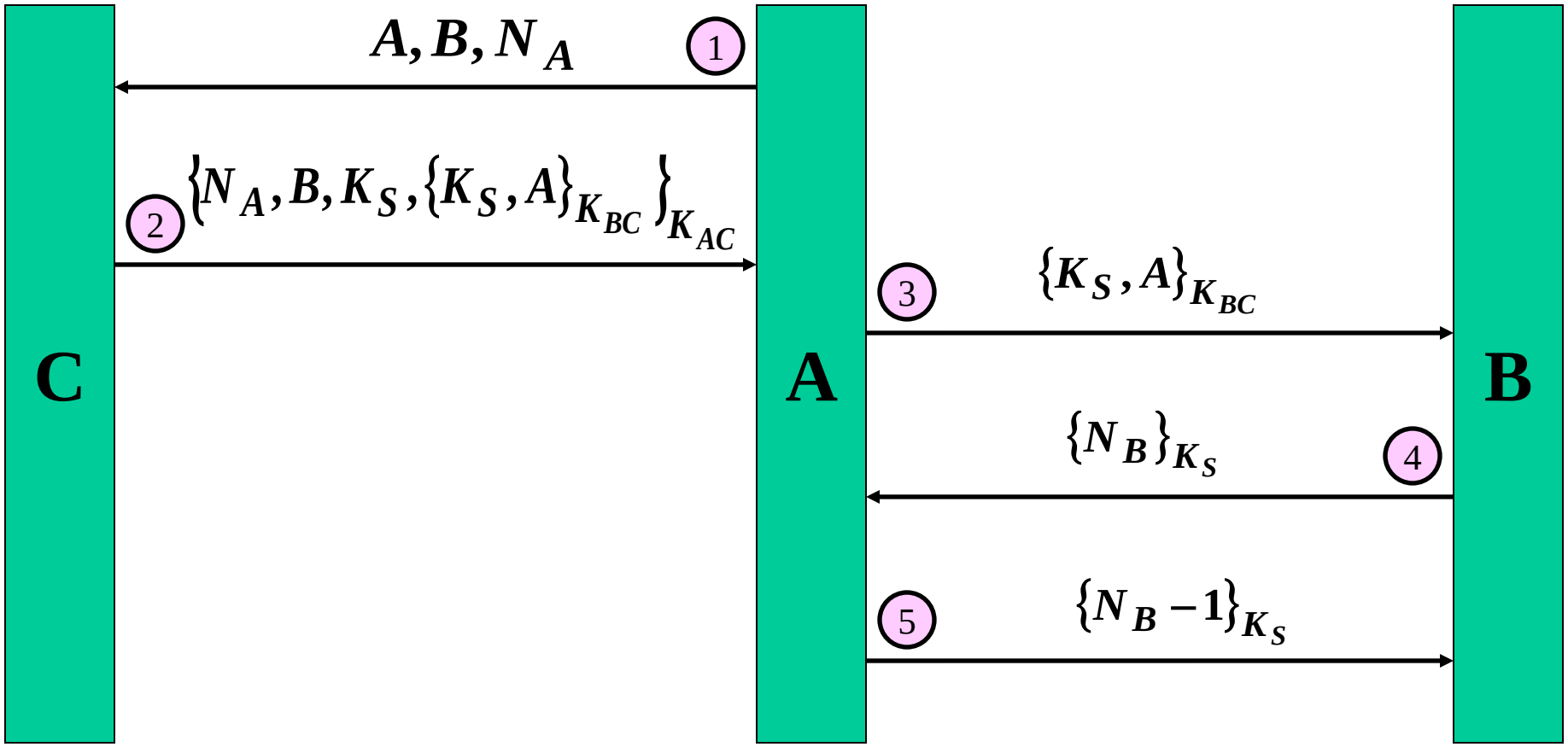
پروتکلهای مبتنی بر الگوی PUSH

سناریوی ۲ :



پروتکل Needham-Schroeder

(سناریوی ۱)

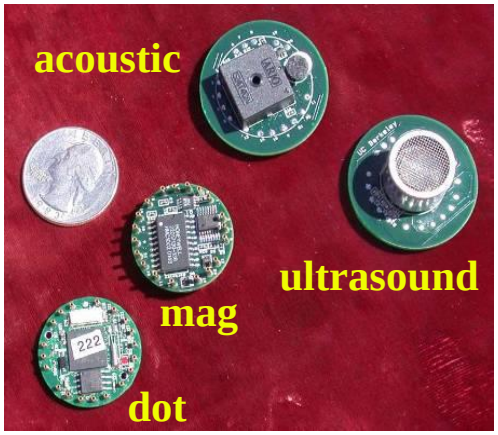


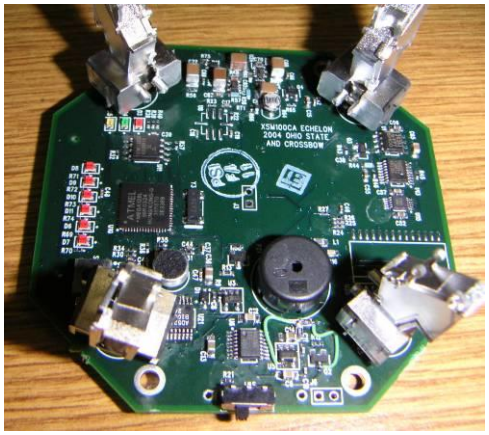
این پروتکل نسبت به **Replay attack** آسیب پذیر است!!!

مدیریت کلید در شبکه های حسگر بی سیم

مقدمه

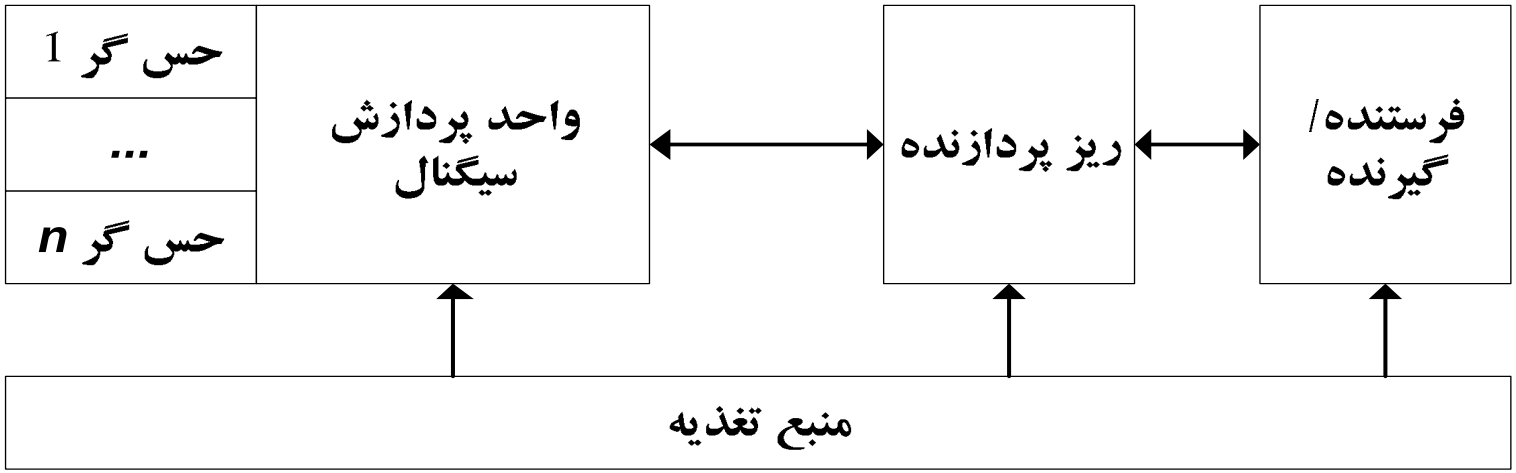
- شبکه‌های حس‌گر نسل جدید شبکه‌های ارتباطی
- متشکل از تعدادی زیاد گره حس‌گر
- جمع آوری اطلاعات محیطی
- استفاده از کانال ارتباطی بی سیم برای ارتباط بین گره‌ها



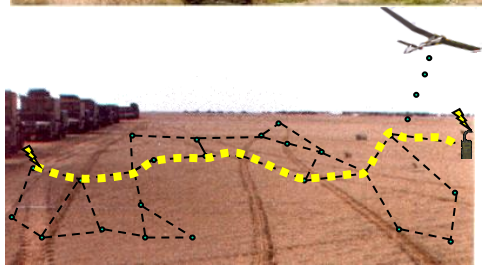


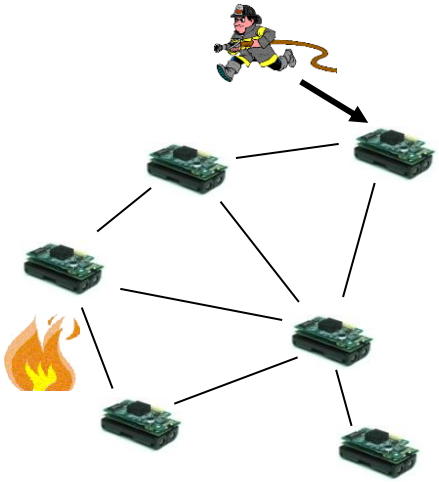
مقدمه

- استفاده از باطری با طول عمر محدود
  - محدودیت در حجم پردازش اطلاعات
  - محدودیت در میزان ارسال و دریافت اطلاعات
- اجزای یک گره حس‌گر



مقدمه





- کاربردهای شبکه‌های حس‌گر بی‌سیم
  - کاربردهای نظامی
    - نظارت بر نیروهای خودی، امکانات و شرایط
    - شناسایی نیروهای دشمن
    - دیده‌بانی در میدان نبرد
    - تشخیص حملات هسته‌ای، میکروبی و شیمیایی
  - کاربردهای زیست محیطی
    - مراقبت از جنگلها و منابع طبیعی

مقدمه

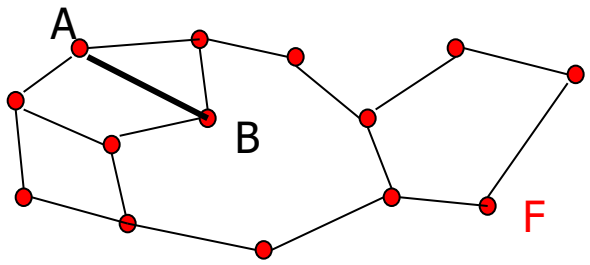
- کاربردهای سلامت
  - مانیتورینگ وضعیت بیماران
- کاربردهای خانگی
  - کاربردهای کنترلی و هوشمند
- کاربردهای علمی
  - بدست آوردن اطلاعات مکانهای صعب العبور و پر خ

مقدمه

- نیازمندی‌های امنیتی
  - محرمانگی : محرمانگی اطلاعات مورد مبادله بین حس‌گرها
  - احراز اصالت : اطمینان از هویت واقعی مبدا اطلاعات
  - توسعه پذیری : امکان افزودن گره‌ها به شبکه بدون اخلال امنیتی در عملکرد شبکه
- مدیریت کلید راه کاری برای دستیابی به سرویس‌های امنیتی

مقدمه

- مدلهای توزیع حس‌گرها در شبکه
  - توزیع تصادفی یکنواخت
    - عدم امکان بهره‌گیری از اطلاعات استقرار حس‌گرها
  - توزیع تصادفی غیر یکنواخت
    - توزیع گروهی حس‌گرها
    - در اختیار بودن احتمال حضور گره‌های حس‌گر در کنار هم

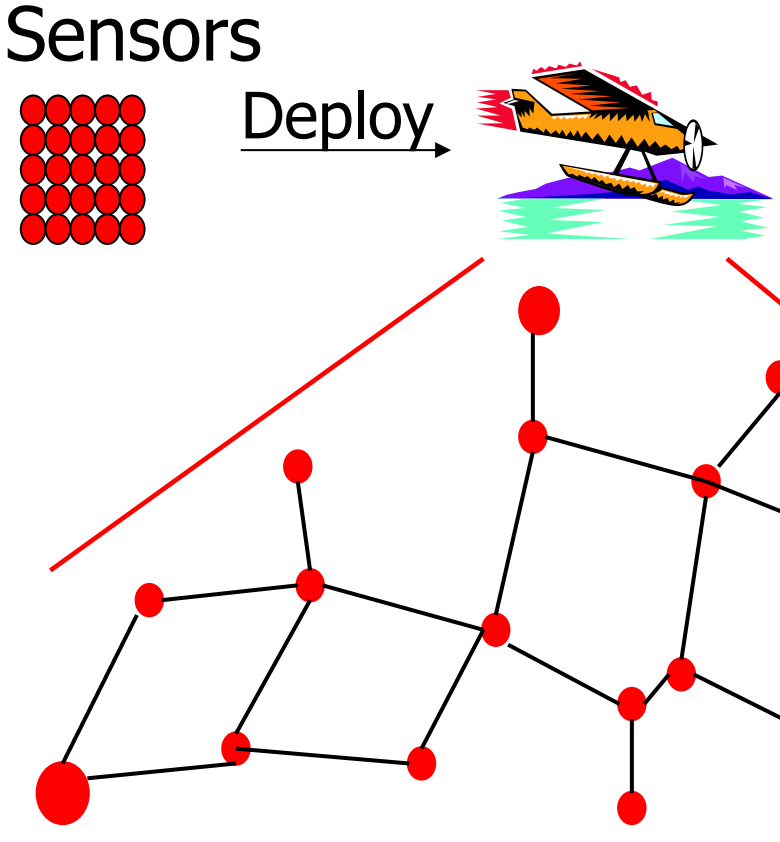


توزیع یکنواخت: Pr(A, B) = Pr(A, F)

توزیع غیر یکنواخت Pr(A, B) >> Pr(A, F)

مقدمه

- توزیع غیر یکنواخت
  - افراز شبکه به سلولهای هم اندازه



✓ **محدود شدن اطلاعات مورد نیاز از شبکه**

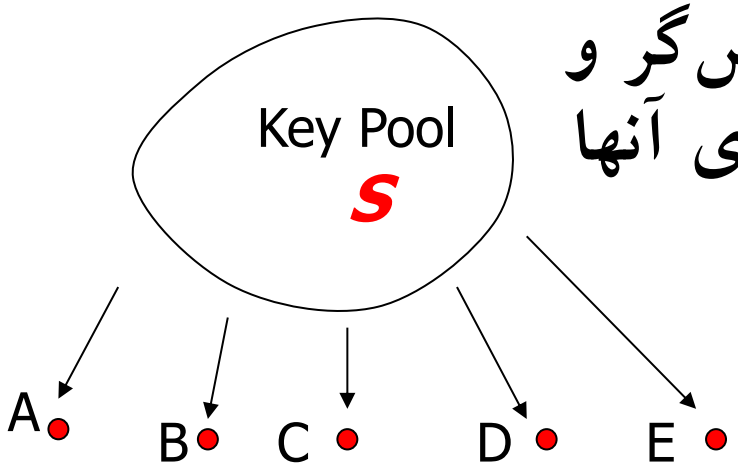
❖ **صرفه‌جویی در مصرف حافظه**

پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- روشهای مدیریت کلید
  - روش مبتنی بر مرکز تولید کلید بر خط
    - کارایی پایین در شبکه‌های حس‌گر
  - روش مبتنی بر کلید عمومی
    - سربار پردازشی زیاد
  - پیش توزیع اطلاعات محرمانه
    - ذخیره زوج کلید ارتباطی در دو گره
    - روش تصادفی
    - روش Blom
    - روش چندجمله‌ای‌های متقارن

پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

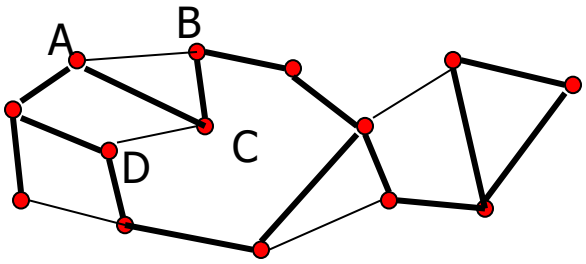
- توزیع کلید تصادفی
  - تولید تعداد زیادی کلید (S) توسط مرکز به عنوان استخر کلید



✓ **انتخاب k کلید تصادفی برای هر حس‌گر و ذخیره آنها در گره‌ها به همراه شناسه‌ی آنها**

پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- تولید کلید بین گره‌ها
  - تولید کلید مستقیم بین دو گره
    - تبادل شناسه‌های کلیدهای ذخیره شده در دو گره به یکدیگر



  - تولید کلید غیر مستقیم بین گره‌ها
    - امکان عدم وجود کلید مشترک بین دو گره
    - استفاده از گره و یا زنجیره‌ای از گره‌ها برای تولید کلید مشترک

پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- **افزایش کارایی پروتکل**

$$1-\binom{S-k}{k}\Big/\binom{S}{k}$$

- **کاهش امنیت کلیدهای ارتباطی بین گره‌ها**

$$1-\left(1-\frac{k}{S}\right)^{X}$$

اندازه استخر کلید S

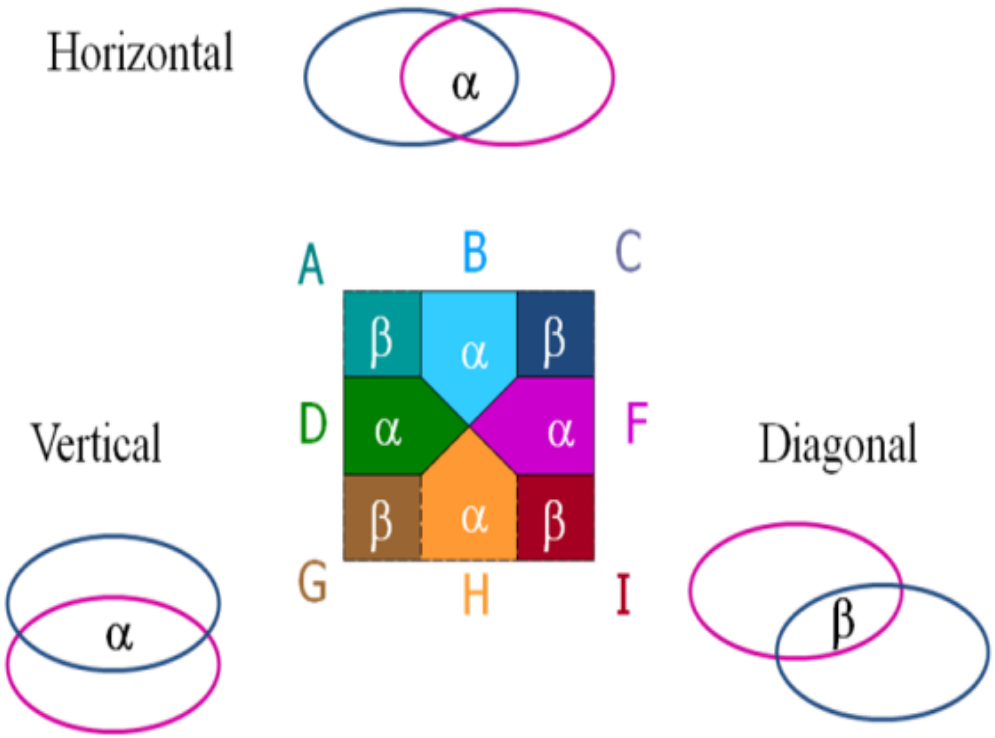
تعداد کلید ذخیره شده k

پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- توزیع کلید تصادفی : ویژگی‌ها
  - ساده
  - بار محاسباتی کم
  - توسعه پذیر
  - بده بستان بین حافظه مصرفی، امنیت و کارآمدی
  - استفاده از یک کلید برای ارتباطات مختلف
    - عدم دستیابی به احراز اصالت بین گره‌ها و امنیت کامل
    - امنیت کامل : عدم امکان افشای کلید مشترک دو گره تسخیر نشده حتی با تسخیر تعدادی زیادی گره

پروتکل مدیریت کلید مبتنی بر توزیع کلید تصادفی

- پروتکل Du-1
  - افراز ناحیه تحت پوشش به نواحی مربعی



- ✓ **اختصاص یک استخر کلید به اندازه S به هر سلول**
- ✓ **قرار گرفتن تعدادی کلید مشترک در استخرهای کلید دو سلول مجاور**

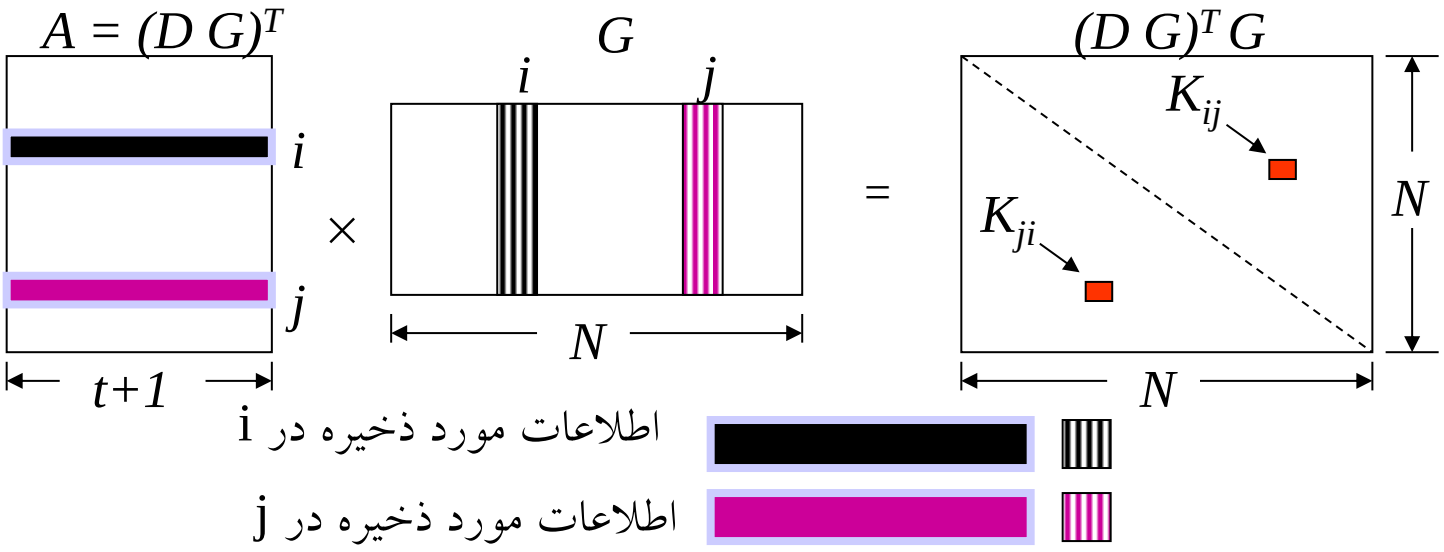
پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- روش Blom
  - تولید ماتریس مولد G بر روی میدان متناهی $GF(q)$
    - N تعداد گره، t سطح امنیت
    - اعلام ماتریس G به صورت عمومی در شبکه
  - تولید ماتریس محرمانه متقارن D $[G]_{t+1\times N}$
  - تولید ماتریس متقارن K با ابعاد $N \times N$ به صورت زیر $[D]_{t+1\times t+1}$

$$K = (D.G)^T .G$$

پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- روش Blom : ادامه
  - درایه (i,j) ماتریس K به عنوان کلید ارتباطی بین گره i و j
    - ذخیره سطر i ام از ماتریس A در گره i
    - ذخیره ستون i ام از ماتریس G در گره i



پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- روش Blom : ادامه
  - تولید کلید مشترک بین گره i و j
    - تبادل ستون ذخیره شده از ماتریس G به یکدیگر
    - ضرب ستون گره مقابل با سطر ذخیره شده از ماتریس A

$$K_{i,j} = [A_{i,1} \quad A_{i,2} \quad \dots \quad A_{i,t+1}] \times \begin{bmatrix} G_{1,j} \\ G_{2,j} \\ . \\ G_{t+1,j} \end{bmatrix}$$

$$K_{j,i} = [A_{j,1} \quad A_{j,2} \quad \dots \quad A_{j,t+1}] \times \begin{bmatrix} G_{1,i} \\ G_{2,i} \\ . \\ G_{t+1,i} \end{bmatrix}$$

پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- روش Blom : ویژگی‌ها
  - امنیت از سطح t
    - در صورت مستقل خطی بودن هر $t+1$ سطر ماتریس G
    - امکان دسترسی به امنیت کامل
    - نیاز به پردازش ضرب ماتریسی در گره‌ها

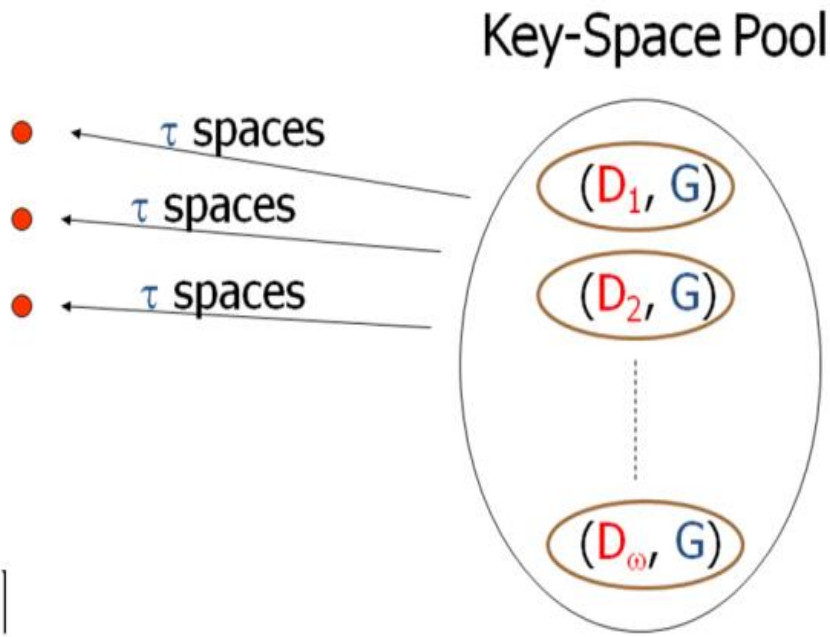
پروتکل مدیریت کلید مبتنی بر Blom

- پروتکل Du-2

✓ **تولید تعدادی زیادی ماتریس D**

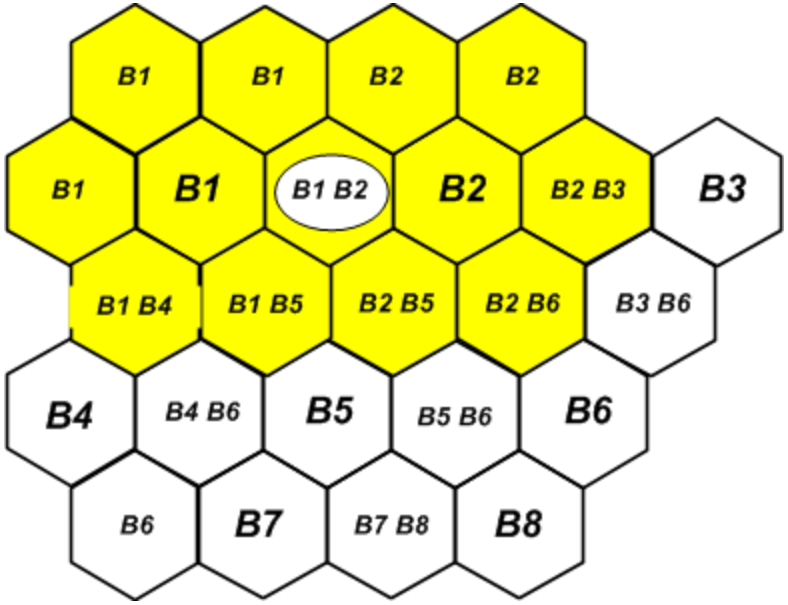
✓ **اختصاص Sc ماتریس به هر سلول**

✓ **انتخاب تصادفی T ماتریس توسط هر گره**



پروتکل مدیریت کلید مبتنی بر Blom

- پروتکل Yu
  - افراز ناحیه تحت پوشش به سلولهای شش گوش
  - اختصاص یک ماتریس Blom به هر سلول
  - اختصاص یک ماتریس Blom به یک سلول مرکزی به همراه شش همسایه‌اش
  - امکان تولید کلید مشترک بین هر سلول با تعداد زیادی از سلول‌های مجاورش



پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- چند جمله‌ای متقارن

– چند جمله‌ای $k+1$ متغیره از متغیرهای $x_1, x_2, \ldots, x_{k+1}$ از درجه t

$$f(x_1, x_2, \ldots, x_{k+1}) = \sum_{i_1=0}^{t} \sum_{i_2=0}^{t} \cdots \sum_{i_{k+1}=0}^{t} a_{i_1, i_2, \cdots i_k, i_{k+1}} x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k} x_{k+1}^{i_{k+1}}$$

– عدم تغییر در حاصل چند جمله‌ای با اعمال هر جایگشت بر روی متغیرها

$$f(x_1, x_2, \ldots, x_{k+1}) = f(x_{\partial(1)}, x_{\partial(2)}, \ldots, x_{\partial(k+1)})$$

پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- چند جمله‌ای متقارن
  - هر گره دارای یک شناسه k بعدی $ID_{Sensor} = (I_1, I_2, ..., I_k)$
  - محاسبه سهم هر گره با استفاد از چند جمله‌ای متقارن و شناسه گره

$$f(I_1, I_2, ..., I_k, x_{k+1}) = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}...\sum_{i_{k+1}=0}^{t} a_{i_1, i_2, ..., i_k, i_{k+1}} I_1^{i_1} I_2^{i_2} ... I_k^{i_k} x_{k+1}^{i_{k+1}} = \sum_{i_{k+1}}^{t} b_{i_{k+1}} x_{k+1}^{i_{k+1}}$$

  - ذخیره ضرائب $b_{i_{k+1}}$ و شناسه گره در حس‌گر

$$b_{i_{k+1}} = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}...\sum_{i_k=0}^{t} a_{i_1, i_2, ..., i_k, i_{k+1}} I_1^{i_1} I_2^{i_2} ... I_k^{i_k}$$

پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- چند جمله‌ای متقارن

– تولید کلید مشترک بین هر دو گره‌ای که شناسه آنها فقط در یک بعد اختلاف داشته باشند

- شناسه گره u : $(c_1, c_2, \ldots u_i, \ldots, c_k)$
- شناسه گره v : $(c_1, c_2, \ldots v_i, \ldots, c_k)$
- تبادل شناسه u_i به گره v و بالعکس
- محاسبه کلید مشترک

$$f_u(v_i) = f(c_1, c_2, \ldots u_i, \ldots c_K, v_i) = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}\ldots\sum_{i_k=0}^{t}\sum_{i_{k+1}=0}^{t} a_{i_1,i_2,\ldots i_k,i_{k+1}} c_1^{i_1} c_2^{i_2} \ldots u_i^{i_i} \ldots c_k^{i_k} v_i^{i_{k+1}}$$

$$f_v(u_i) = f(c_1, c_2, \ldots v_i, \ldots c_K, u_i) = \sum_{i_1=0}^{t}\sum_{i_2=0}^{t}\ldots\sum_{i_k=0}^{t}\sum_{i_{k+1}=0}^{t} a_{i_1,i_2,\ldots i_k,i_{k+1}} c_1^{i_1} c_2^{i_2} \ldots v_i^{i_i} \ldots c_k^{i_k} u_i^{i_{k+1}}$$

$K_{u,v}$

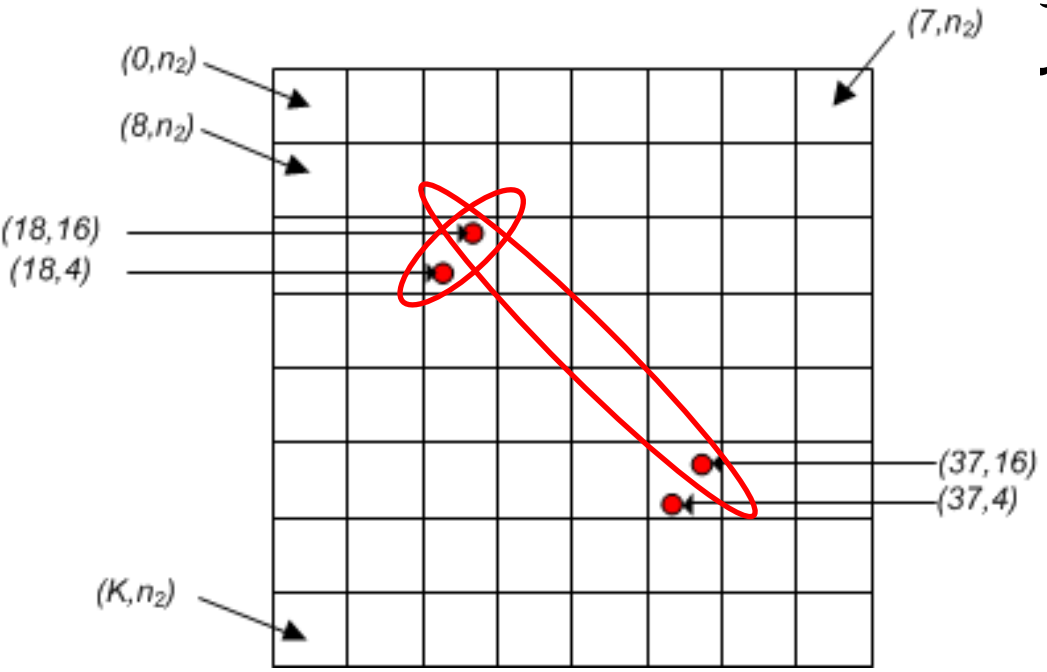
پروتکل‌های پایه مدیریت کلید در شبکه های حس‌گر

- چند جمله‌ای متقارن : ویژگی
  - امنیت کلید ارتباطی بین هر دو گره
    - در صورتی تبانی کمتر از t گره
  - تعیین مقدار t با توجه به سطح امنیت مورد نیاز در کلید ارتباطی دو گره
    - مقدار t برای امنیت کامل در تولید N_i سهم از یک چند جمله‌ای

$$0 \leq N_i - 2 \leq t$$

پروتکل مدیریت کلید مبتنی بر چند جمله‌ای متقارن

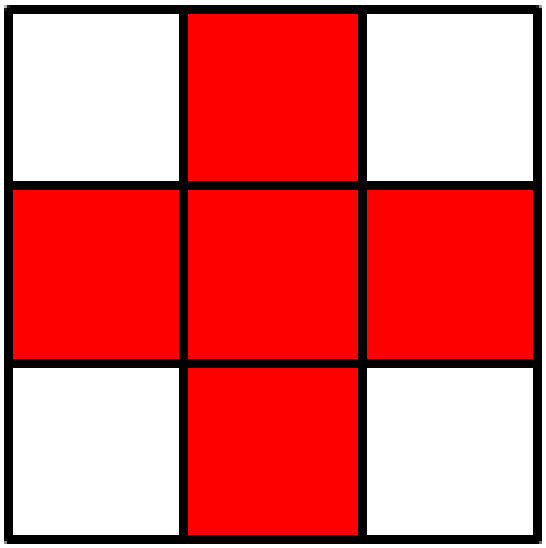
- پروتکل LAKE
  - افراز ناحیه تحت پوشش به سلولهای مربعی
  - اختصاص شناسه دو بعدی (n_1,n_2) به هر گره
    - n_1: شناسه اختصاصی سلول ، n_2: شناسه اختصاصی گره در سلول



- ✓ **تولید سهم با استفاده از چند جمله‌ای متقارن ۳ متغیره از درجه t**
- ✓ **امکان تولید کلید مشترک بین گره‌های مختلف**

پروتکل مدیریت کلید مبتنی بر چند جمله‌ای متقارن

- پروتکل LPBK
  - اختصاص چند جمله‌ای‌های متفاوت به هر سلول
  - تولید سهم برای گره‌های یک سلول به همراه گره‌های متعلق به سلول‌های همسایه افقی و عمودی
    - هر گره دارای ۵ سهم
    - تولید سهم برای ۵ سلول توسط هر کدام از چند جمله‌ای‌ها



Secret Sharing Algorithms

What is secret sharing?

- In cryptography, **secret sharing** refers to a method for distributing a secret amongst a group of participants, each of which is allocated a *share* of the secret.
- The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.

Why do we need secret sharing?

- Gives tight control and removes single point vulnerability.

- Individual key share holder cannot change/access the data.

Mathematical Definition

- Goal is to divide some data *D* (e.g., the safe combination) into n pieces D1,D2….Dn in such a way that:
  - Knowledge of any k or more D pieces makes D easily computable.
  - Knowledge of any k -1 or fewer pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).
- This scheme is called (k,n) threshold scheme. If k=n then all participants are required together to reconstruct the secret.

Shamir's Secret Sharing

- Suppose we want to use (k,n) threshold scheme to share our secret S where $k < n$.
- Choose at random (k-1) coefficients a1,a2,a3…ak-1 , and let S be the a0

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{k-1}^{k-1}$$

Shamir's Secret Sharing

- Construct n points (i,f(i)) where i=1,2…..n

- Given any subset of k of these pairs, we can find the coefficients of the polynomial by interpolation, and then evaluate a0=S , which is the secret.

Example

- Let S=1234
- n=6 and k=3 and obtain random integers

  a1=166 and a2=94

$$f(x) = 1234 \quad + 166x + 94x^2$$

- Secret share points

  (1,1494),(2,1942)(3,2598)(4,3402)(5,4414)(6,5614)

- We give each participant a different single point (both x and f(x)).

Reconstruction

- In order to reconstruct the secret any 3 points will be enough
- Let us consider

$$(x_0, y_0) = (2,1924), (x_1, y_1) = (4,3402), (x_2, y_2) = (5,4414)$$

U sin *gLagrangepolynomials*

$$l_0 = x - x_1 / x_0 - x_1 * x - x_2 / x_0 - x_2 = x - 4/2 - 4 * x - 5/2 - 5 = 1/6x^2 - 11/2x + 31/3$$

$$l_1 = x - x_0 / x_1 - x_0 * x - x_2 / x_1 - x_2 = x - 2/4 - 2 * x - 5/4 - 5 = -1/2x^2 - 31/2x - 5$$

$$l_2 = x - x_0 / x_2 - x_0 * x - x_1 / x_2 - x_1 = x - 2/5 - 2 * x - 4/5 - 4 = 1/3x^2 - 2x + 22/3$$

$$f(x) = \sum_{j=0}^{2} y_j l_j(x) = 1942(1/6x^2 - 11/2x + 31/3) + 3402(-1/2x^2 - 31/2x - 5) + 4414(1/3x^2 - 2x + 22/3)$$

$$f(x) = 1234 + 166x + 94x^2$$

Shamir's Secret Sharing (Cont.)

– **Key Recovery Phase:**

①Any t shadows can recover the $h(x)$ by pooling t points $(x_{i_1}, K_{i_1}), (x_{i_2}, K_{i_2}), .., (x_{i_t}, K_{i_t})$

$$h(x) = \sum_{s=1}^{t} K_s \prod_{\substack{j=1 \\ j \neq s}}^{t} \frac{(x - x_{i_j})}{(x_{i_s} - x_{i_j})} \bmod p$$

②$K = h(0)$