

NIS/CpE 691CE

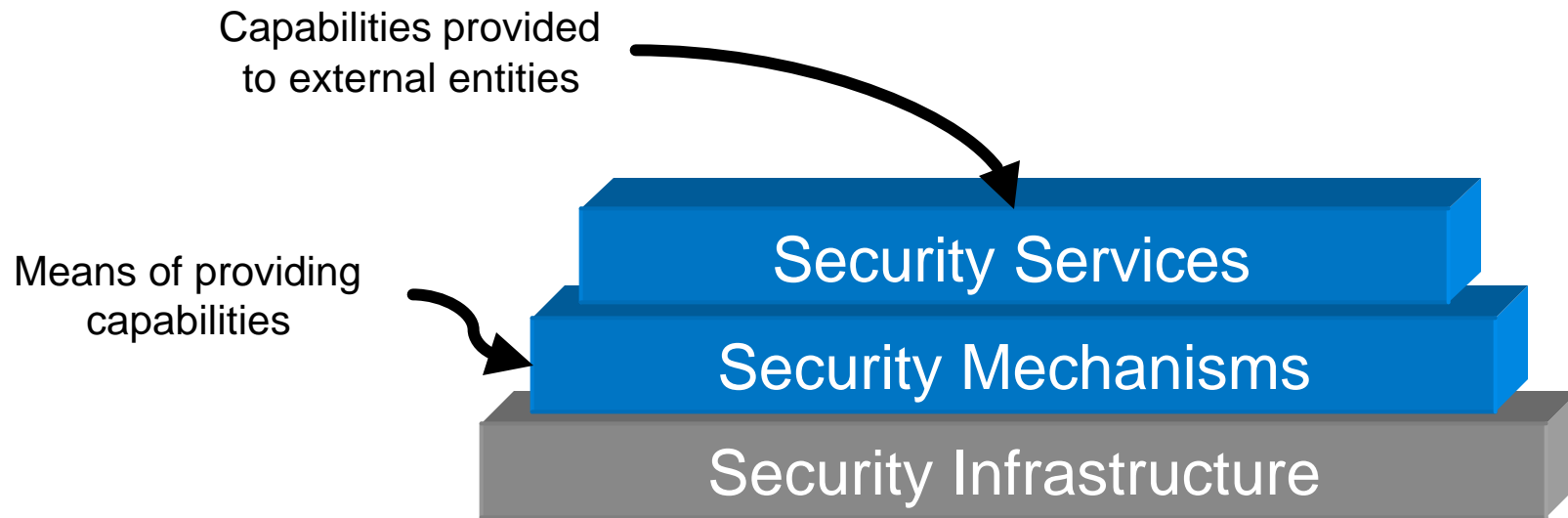
Information System Security

Class 2 – 9/16/02

What Security Issues Can Be Addressed By Cryptography and Related Techniques?

- Cryptography is NOT the solution to all security problems, but
- It does provide an enabling technology for many issues.
- If intelligently applied (balanced against other issues and needs) it can be of substantial value
- It provides a good place to start discussing detailed security technologies in an Information System

From Last Time: One Structured Way of Viewing Security



Categories of Security Mechanisms And Those That Can Be Addressed By Cryptography

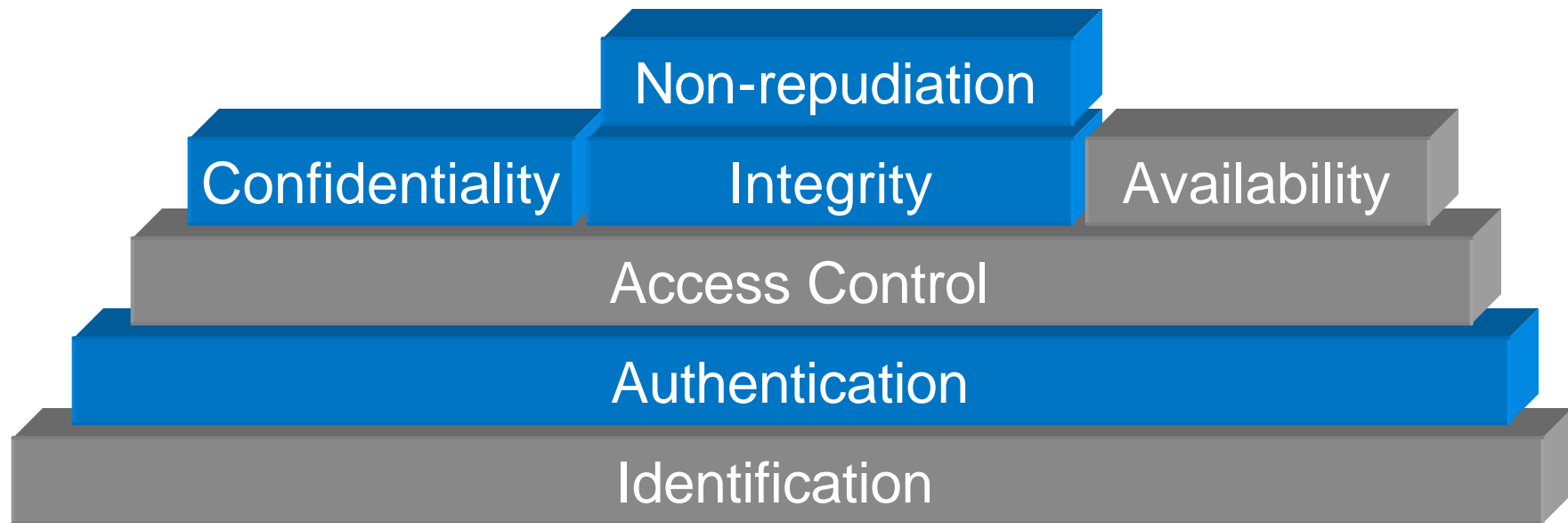
- *Prevent* occurrence of compromise
- *Detect* occurrence compromise
- *Correct* after-effects of compromise

Some Security Mechanisms and the Security Services They Could Enable

Mechanisms: \ Service:	ID	Auth	AC	Conf	Integ	Avail	NR
Cryptography/Encryption		?		?	?		?
Quality of Service Controls						?	
Audit Logs			? *	? *	? *	? *	?
Trusted Software			?	?	?	?	?
Security Policies	?	?	?	?	?	?	?
Biometrics	?	?					
Smart Cards	?	?	?	?	?		?
System Backups					?		?
Security Assessment	?	?	?	?	?	?	?

List of mechanisms is not meant to be exhaustive

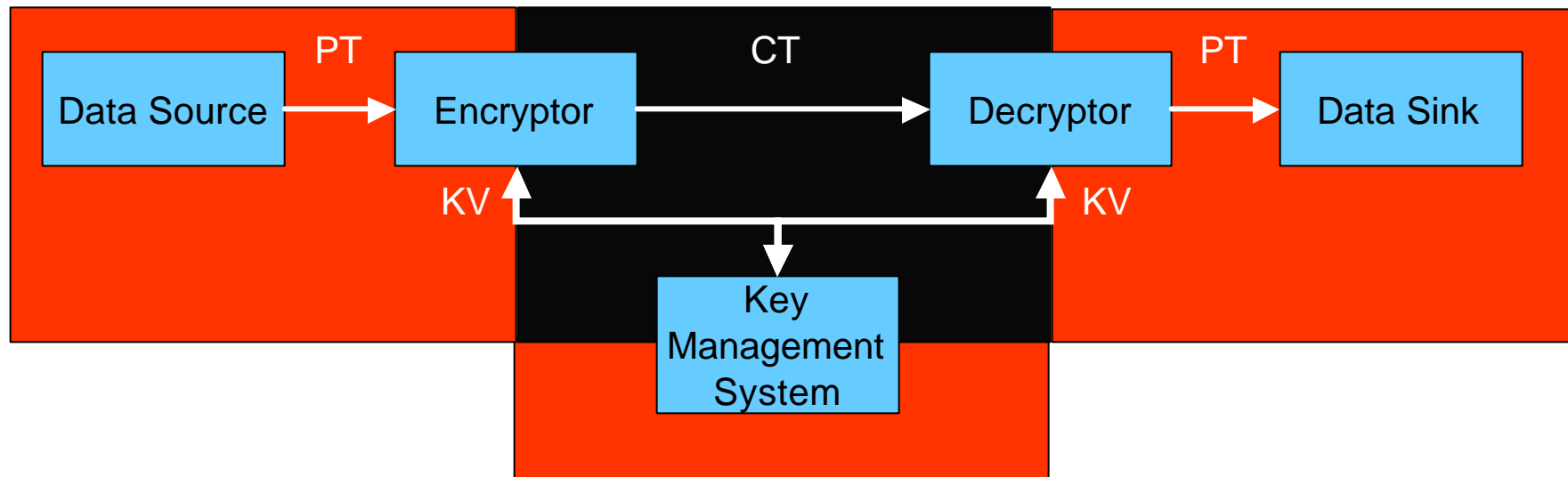
One Structured Way of Viewing Security And Security Services Addressed By Cryptograpy



Security Services

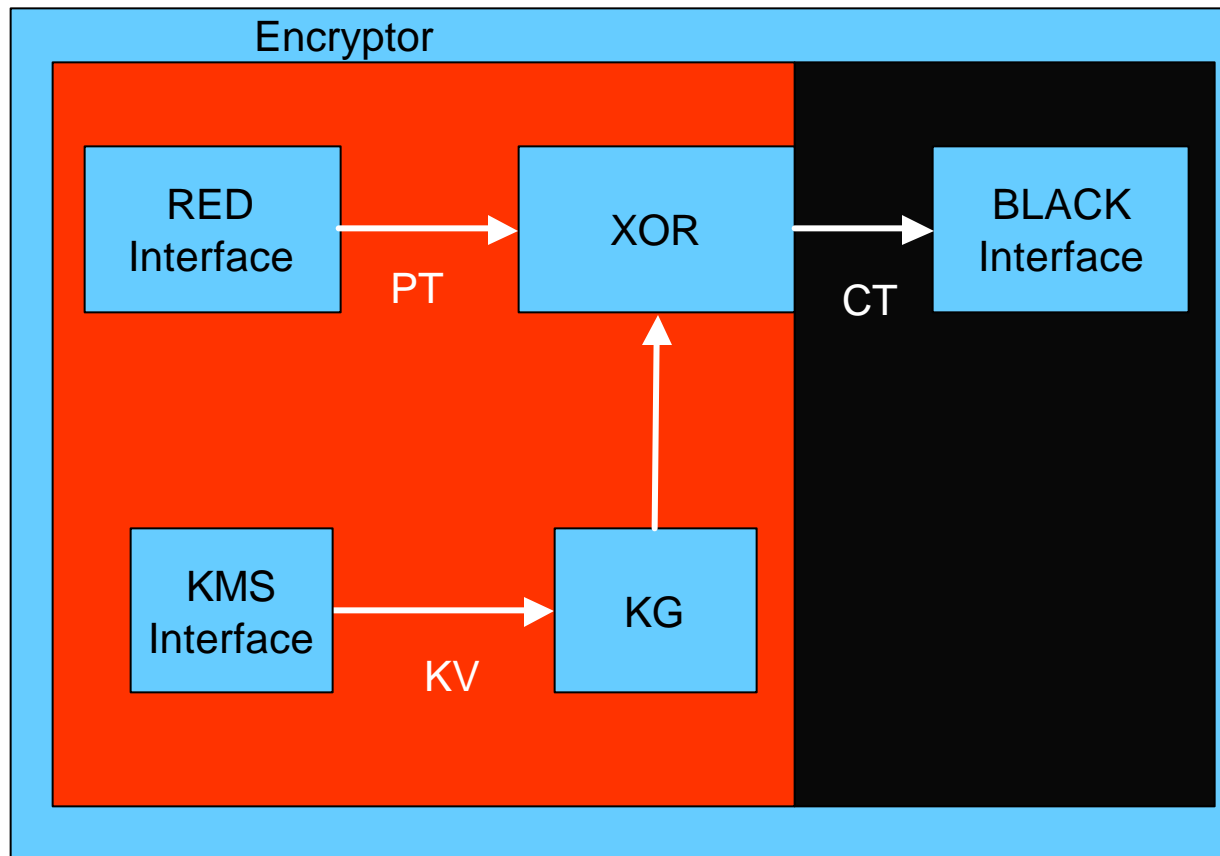
Cryptography Terminology

- Plaintext (PT) – unprotected source material (images, text, data, etc.)
- Ciphertext (CT) – Plaintext that has been enciphered (encrypted)
- Key Variable (KV) – Parameter of cryptographic system that selects, specifies, or controls key stream
- Key Management – Process for providing corresponding key variable(s) to sender and receiver



Cryptography Terminology - Continued

- Key Stream (Key Sequence) (KS) – (Pseudo)random string of symbols used to encrypt and/or decrypt plaintext
- Key Generator (KG) – Device that generates the key stream for a stream encipherment device



Miscellaneous Cryptography Terminology

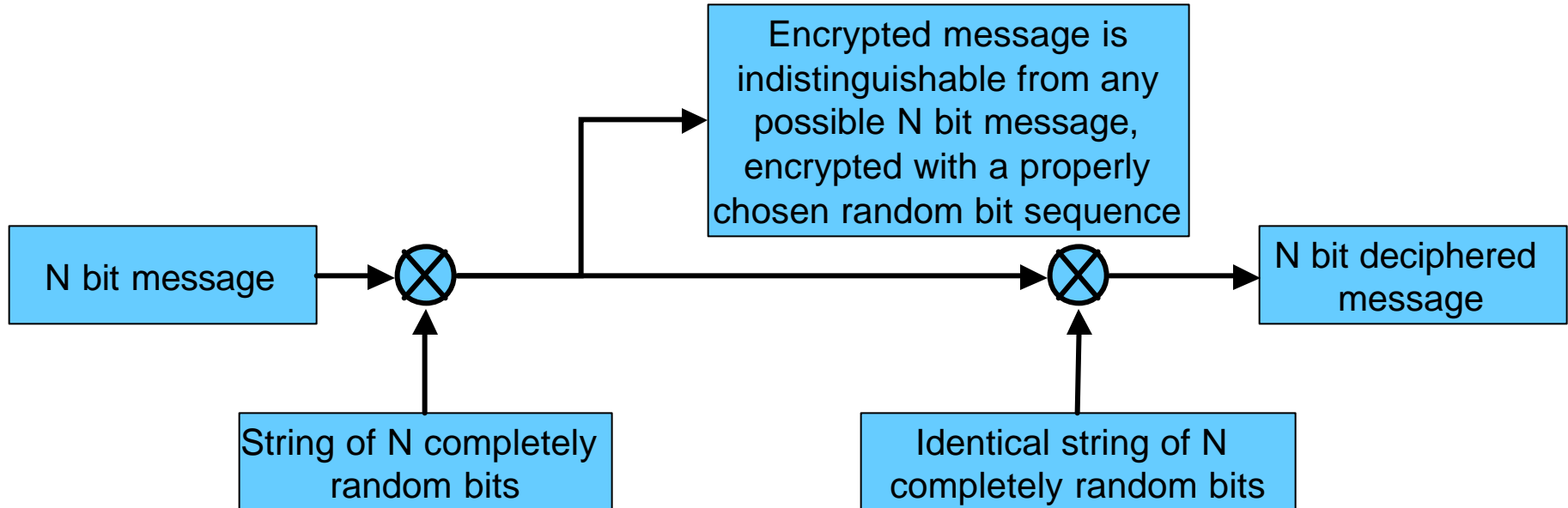
- Affine:
 $F(x) = \alpha x + \beta$
- Linear:
 $F(x) = \gamma x$
 $F(\alpha x + \beta y) = \alpha F(x) + \beta F(y)$ [superposition]
- Nonlinear:
Superposition does not apply
- Permutation:
Reordering of inputs, e.g., $P(\{a,b,c,d\}) = \{c,b,a,d\}$
- Substitution:
Functional mapping, non necessarily 1-1 or onto

Evolution of Cryptography

- Monoalphabetic substitution, e.g.,
 - Caesar cipher {a,b,c,d,e,f,...,x,y,z} -> {b,c,d,e,f,g,...,y,z,a}
 - Atbash cipher {a,b,c,d,e,f,...,x,y,z} -> {z,y,x,w,v,u,t,s,r,q,p,o,n,m,l,k,j,i,h,g,f,e,d,c,b,a}
 - Any permutation of the alphabet
 - Easily solved by observing single and double letter frequencies
 - English (like most other non-ideographic languages) have distinct letter frequencies over a small alphabet.
 - Encoding English letters requires $\log_2(26) \sim 4.7$ bits/letter,
 - but information content in English text is $\sum p \log_2(p)$
With unequal letter probabilities, actual information content is much lower.
Equivocation of source is the effective information content
- Polyalphabetic substitution:
 - thisisamessagetobeencrypted** - plaintext
 - badbadbadbadbadbadbadbadbad** - key stream
 - vimujwcniuteifxqcigogtztvfh** - ciphertext
 - Correlation-like techniques find the length of the key stream, k
 - Problem then reduces to solving k monoalphabetic ciphers
 - Using running text (e.g., from an agreed to book) makes solution harder, but with enough ciphertext, both the plaintext as well as the key stream are easily found

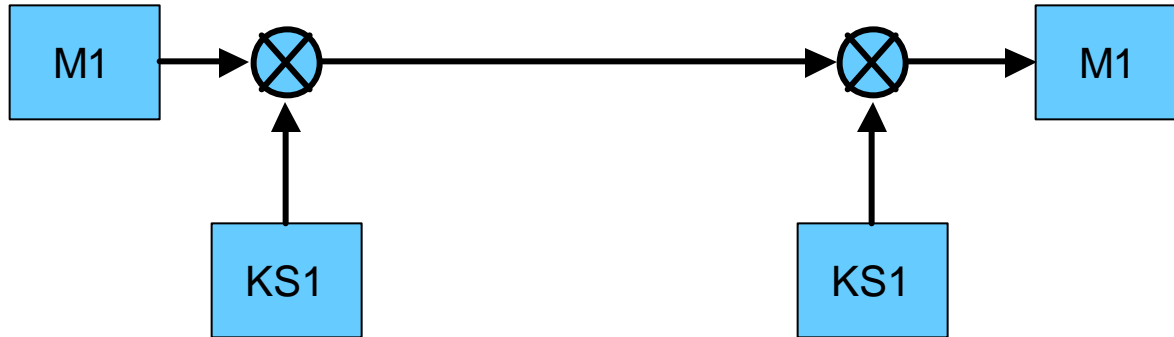
Evolution of Cryptography - 2

- Weakness of polyalphabetic cipher is repetition of the key stream
– What if it never repeated?

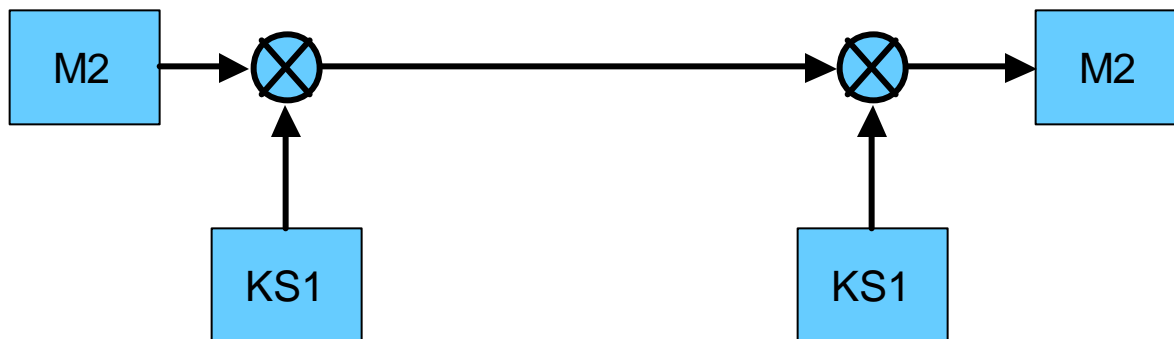


- One-time-pad is the only provably secure cryptographic system
What happens if key sequence is (accidentally) reused?

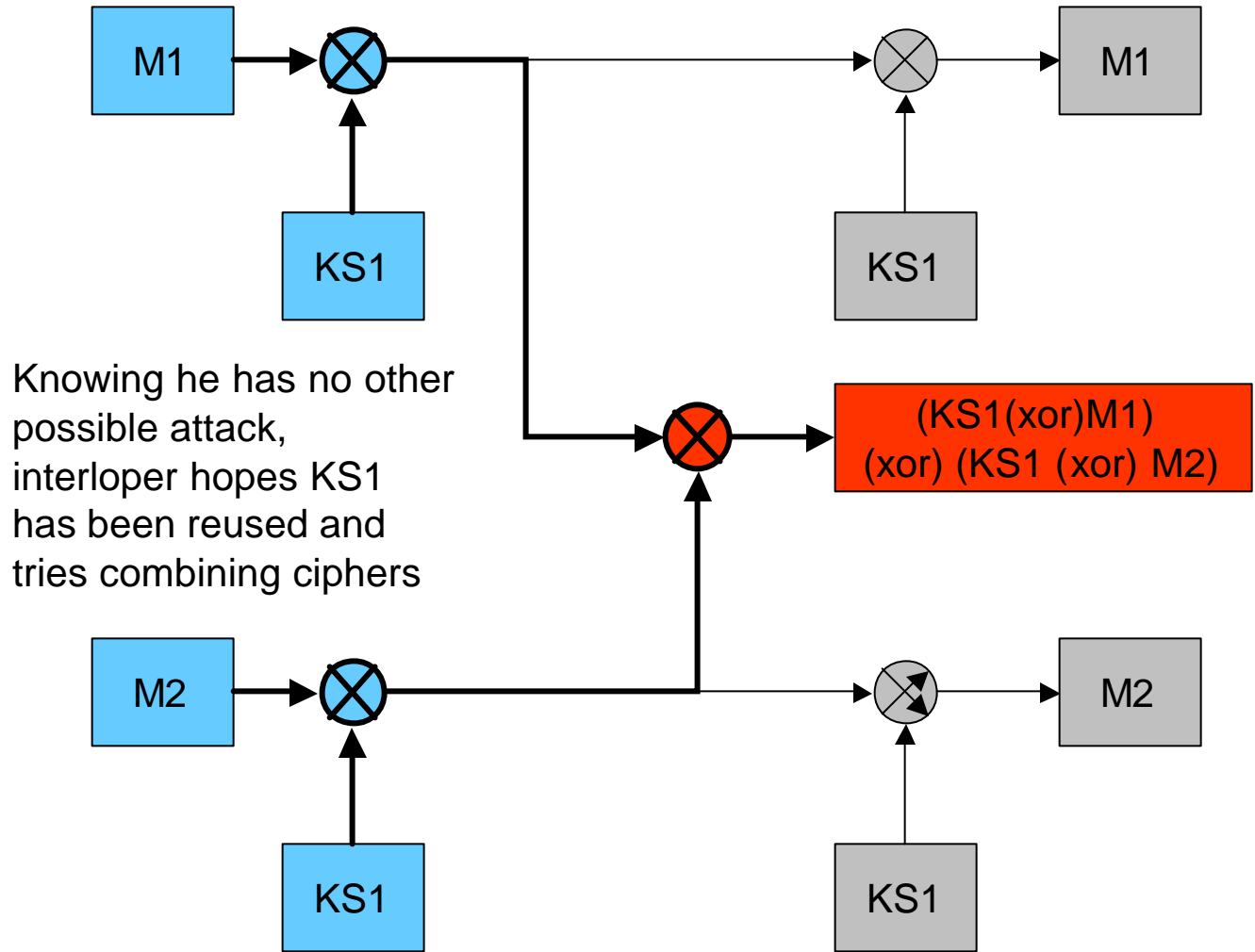
One-bit-pad Key Reuse



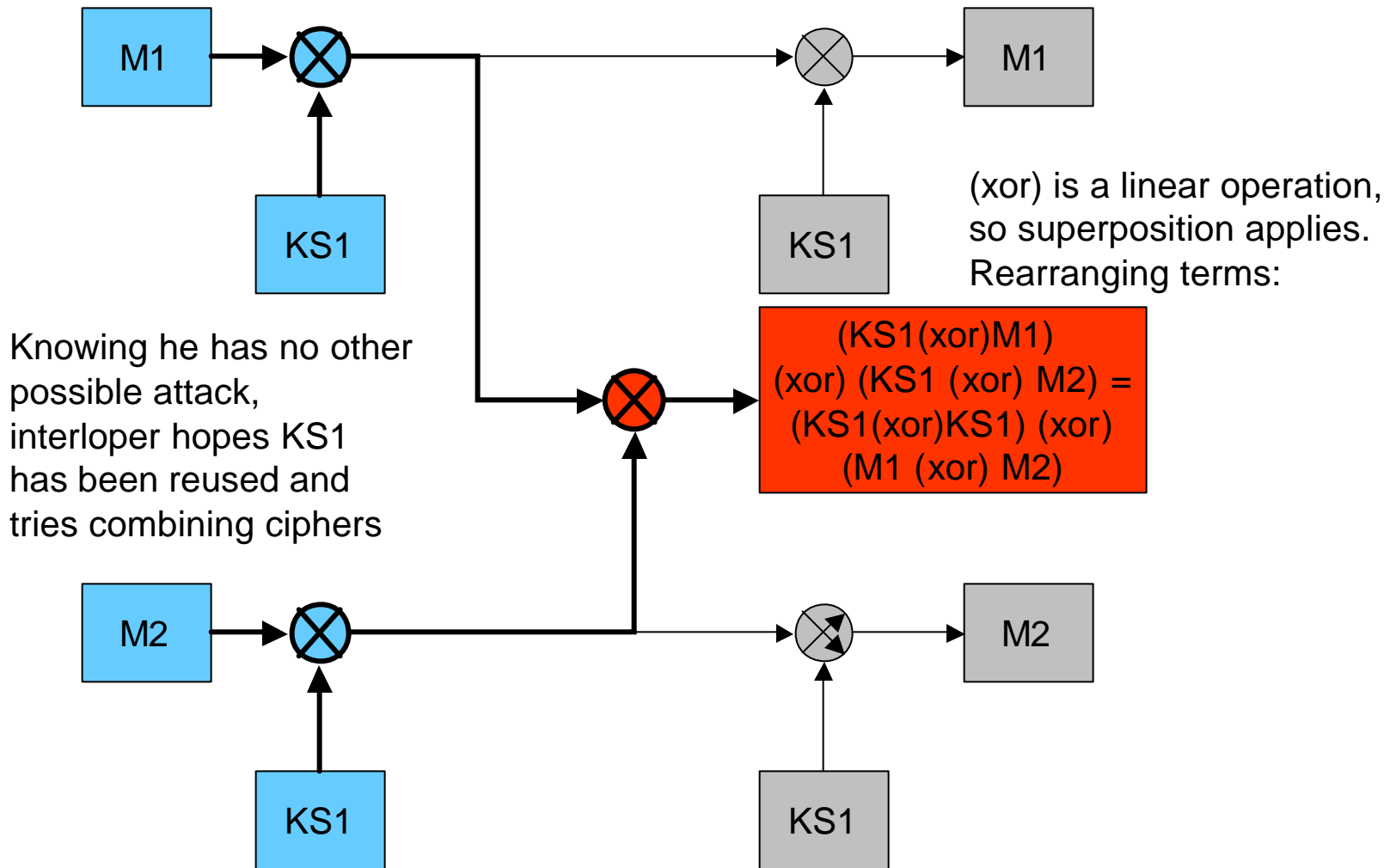
Sender (or receiver) accidentally sent M2, reusing KS1, previously used for M1



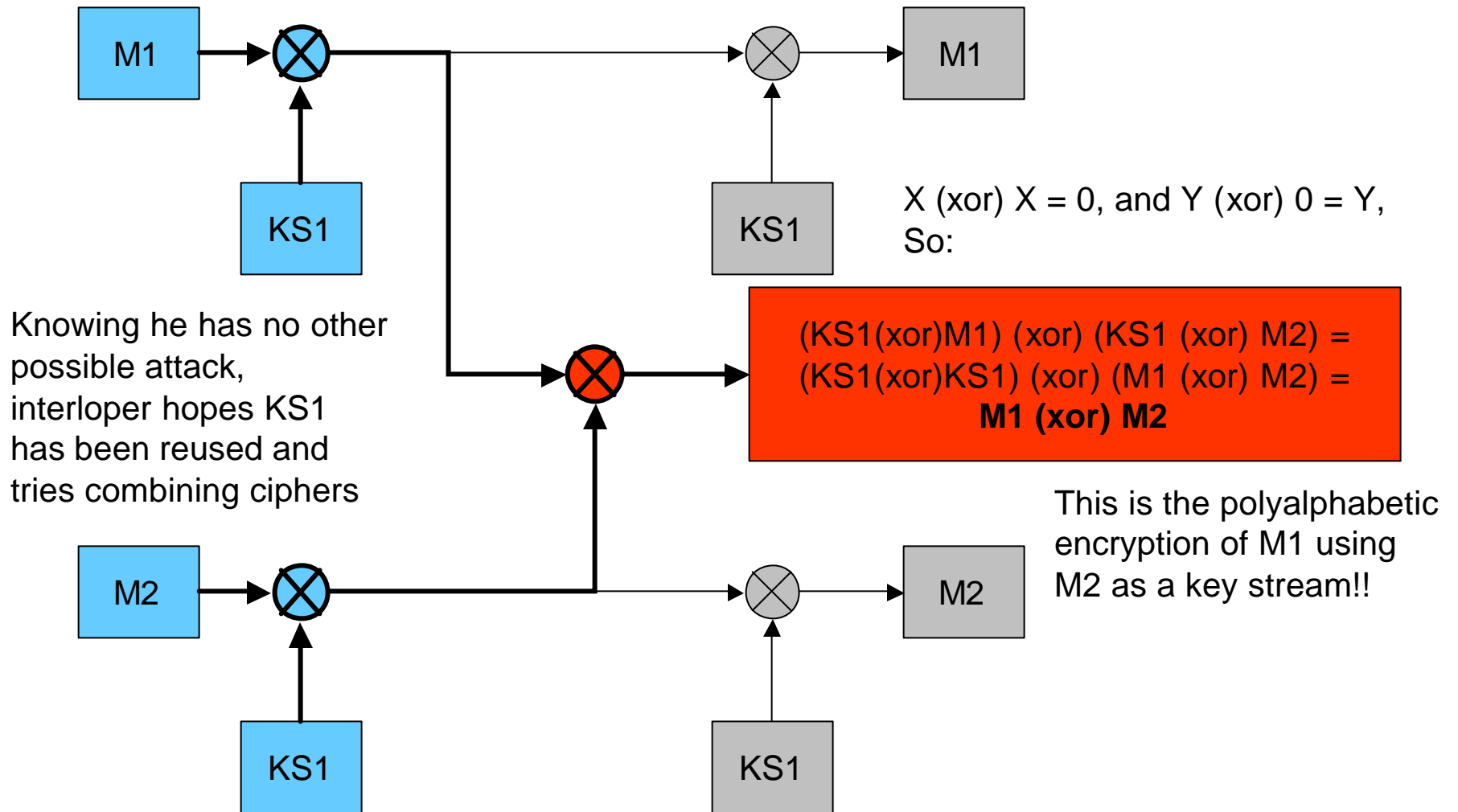
One-bit-pad Key Reuse



One-bit-pad Key Reuse

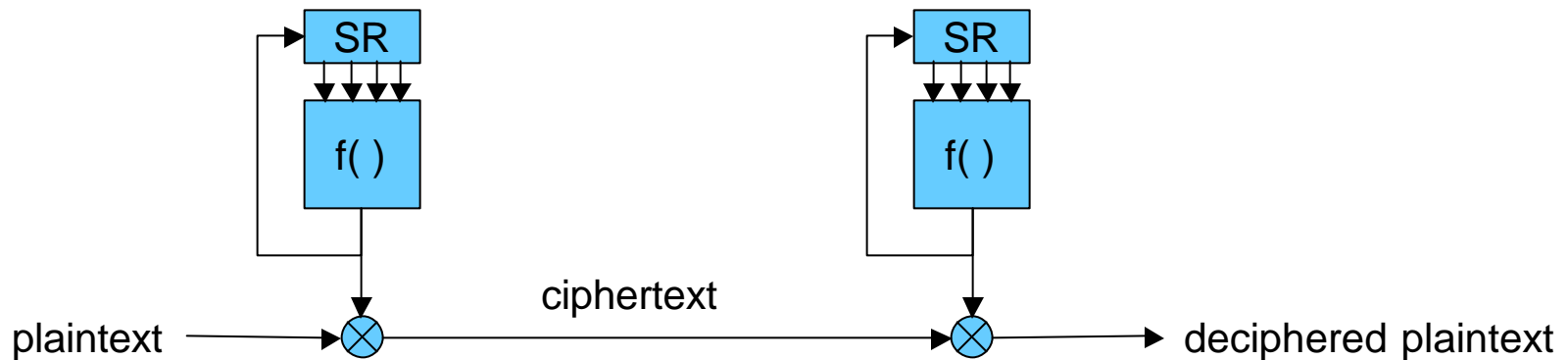
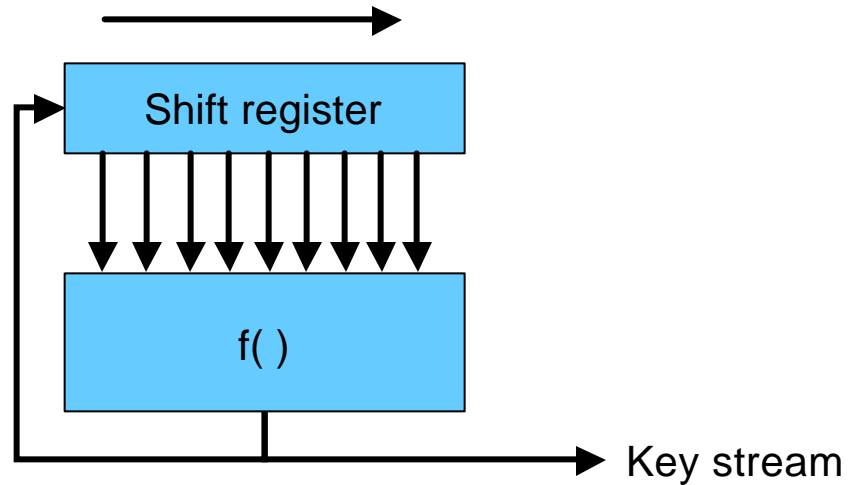


One-bit-pad Key Reuse



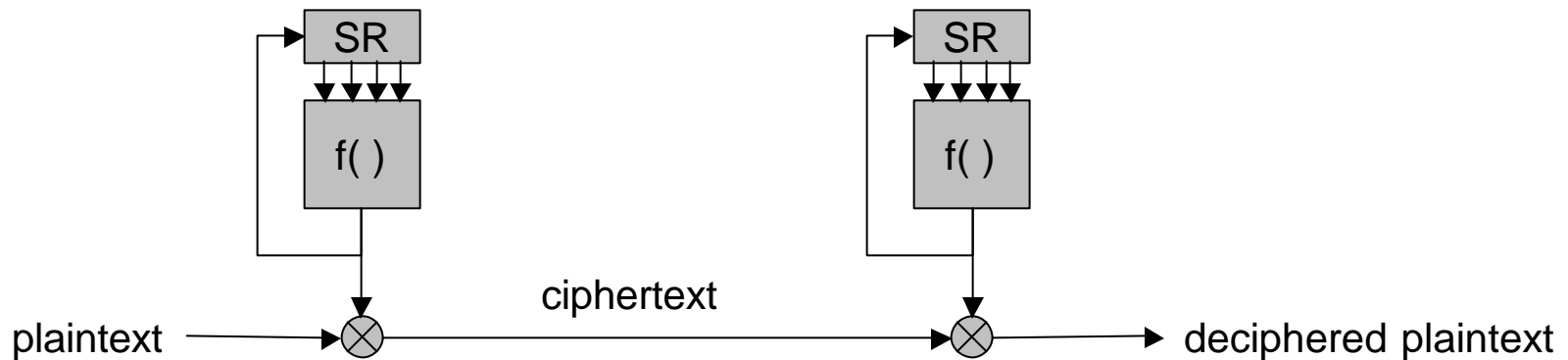
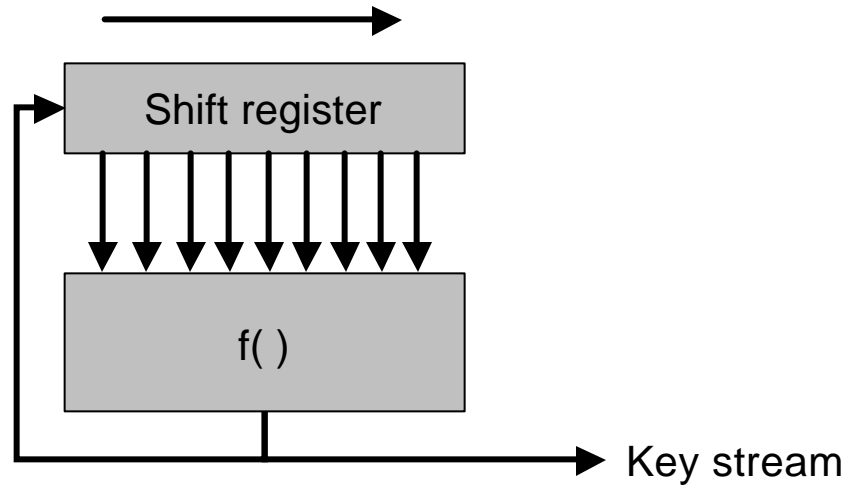
Generating Long Pseudo-Random Sequences

- For N bit register, if $f(x)$ is linear, $2N-1$ bits of key stream are sufficient to find $f()$
- So, $f()$ must be nonlinear



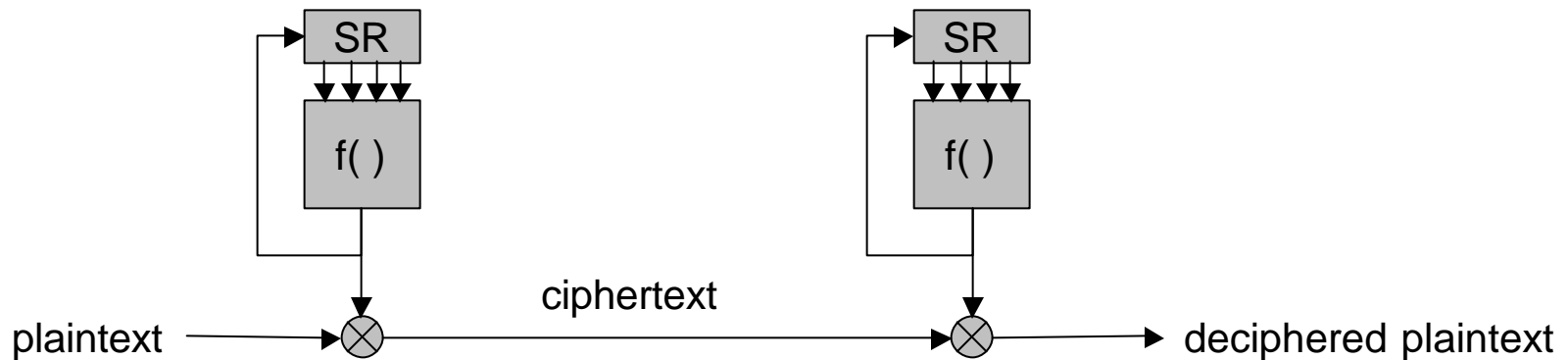
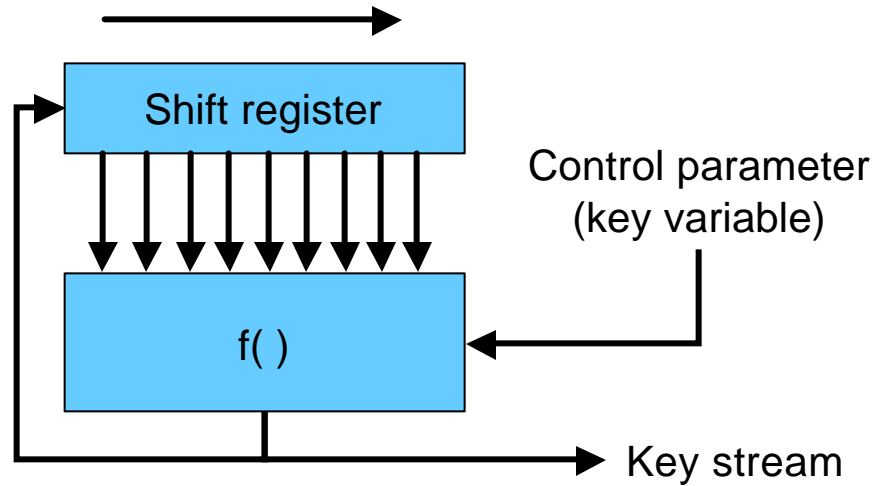
Generating Long Pseudo-Random Sequences

- How to make $f()$ easy to change?
- What about synchronization?



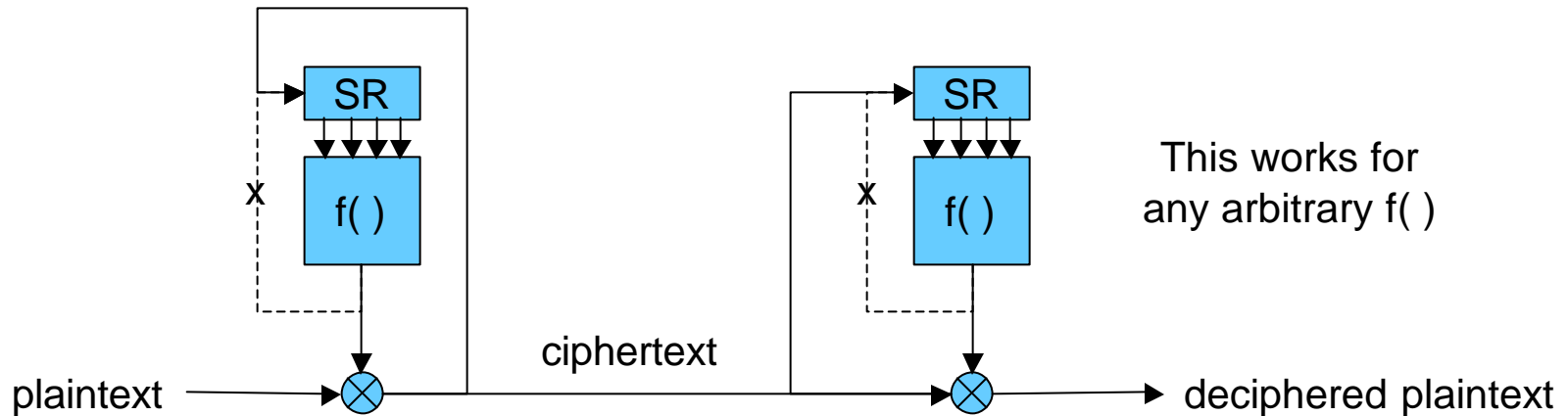
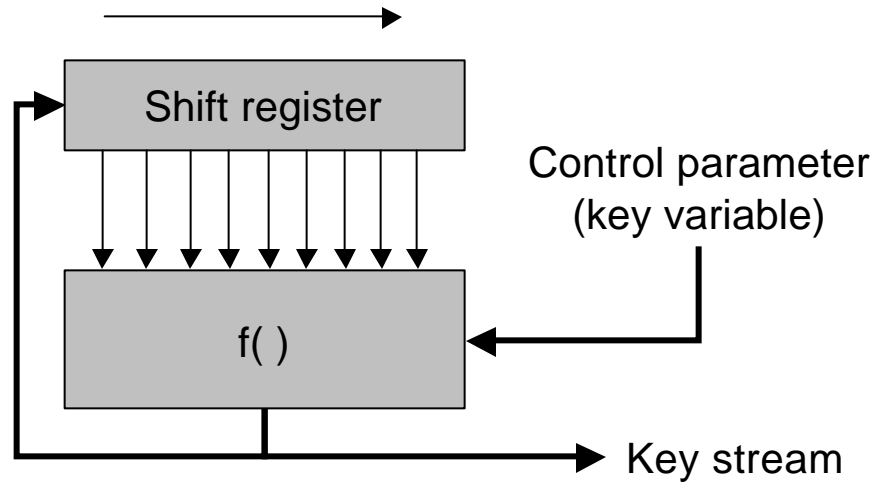
Generating Long Pseudo-Random Sequences

- How to make $f()$ easy to change?
- What about synchronization?

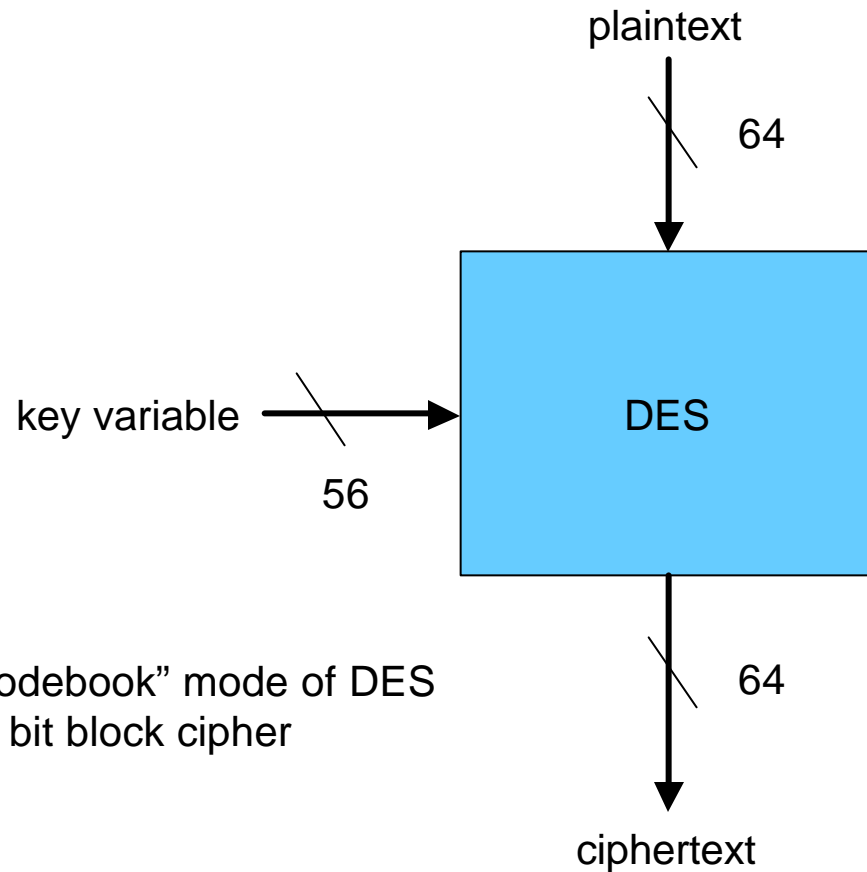


Generating Long Pseudo-Random Sequences

- How to make $f()$ easy to change?
- What about synchronization?

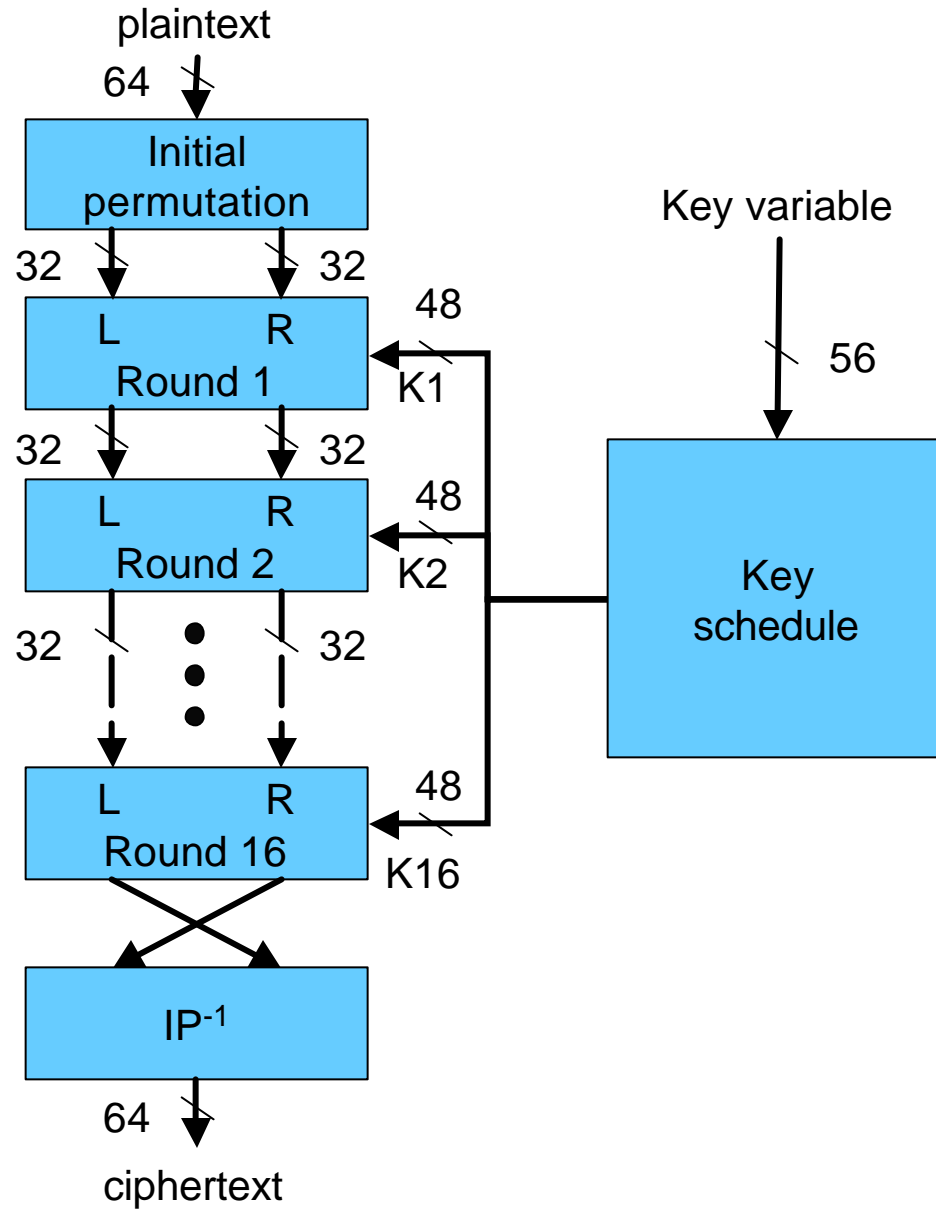


DES as one $f(\)$ option

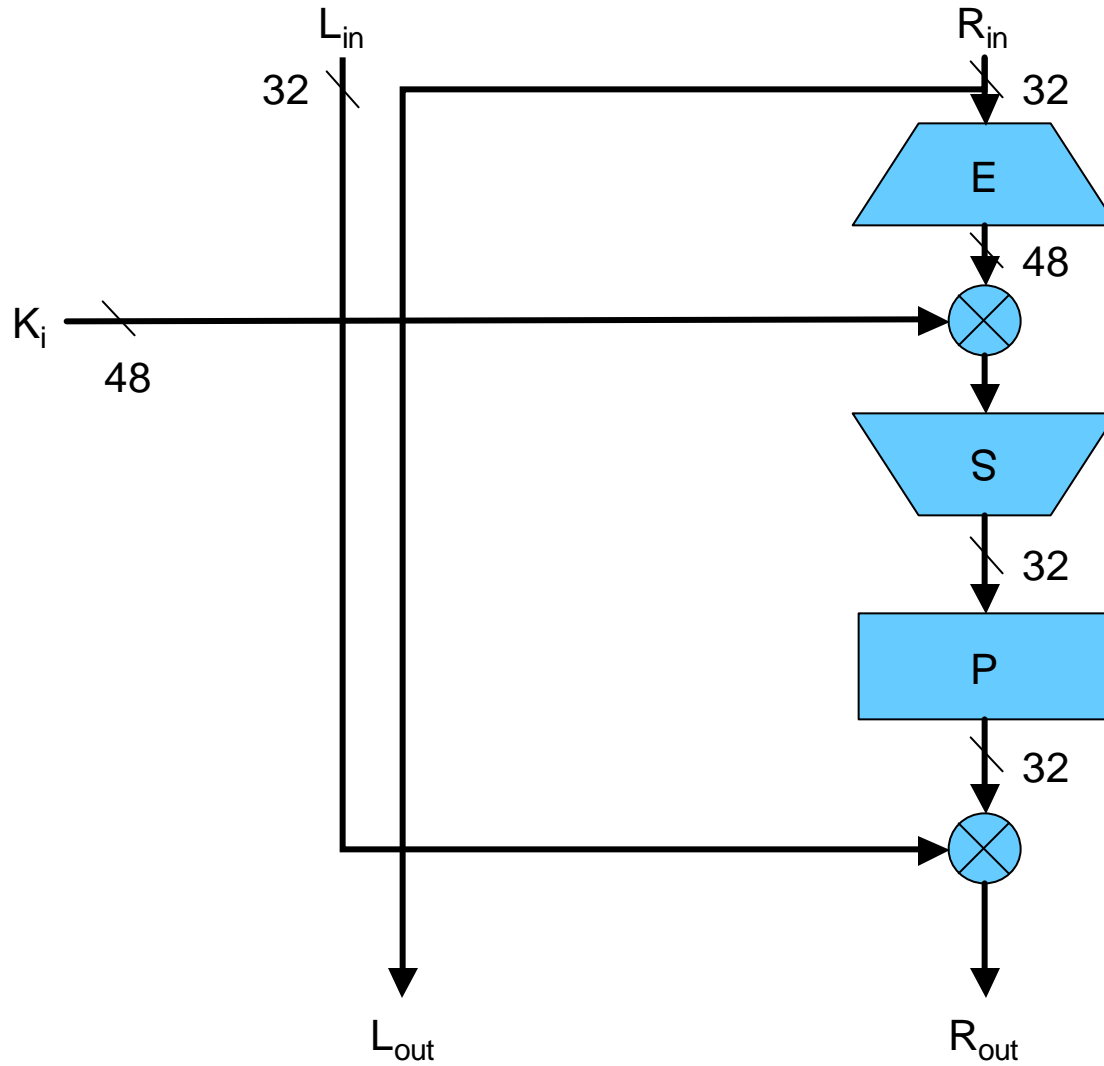


“Electronic codebook” mode of DES
– 64 bit block cipher

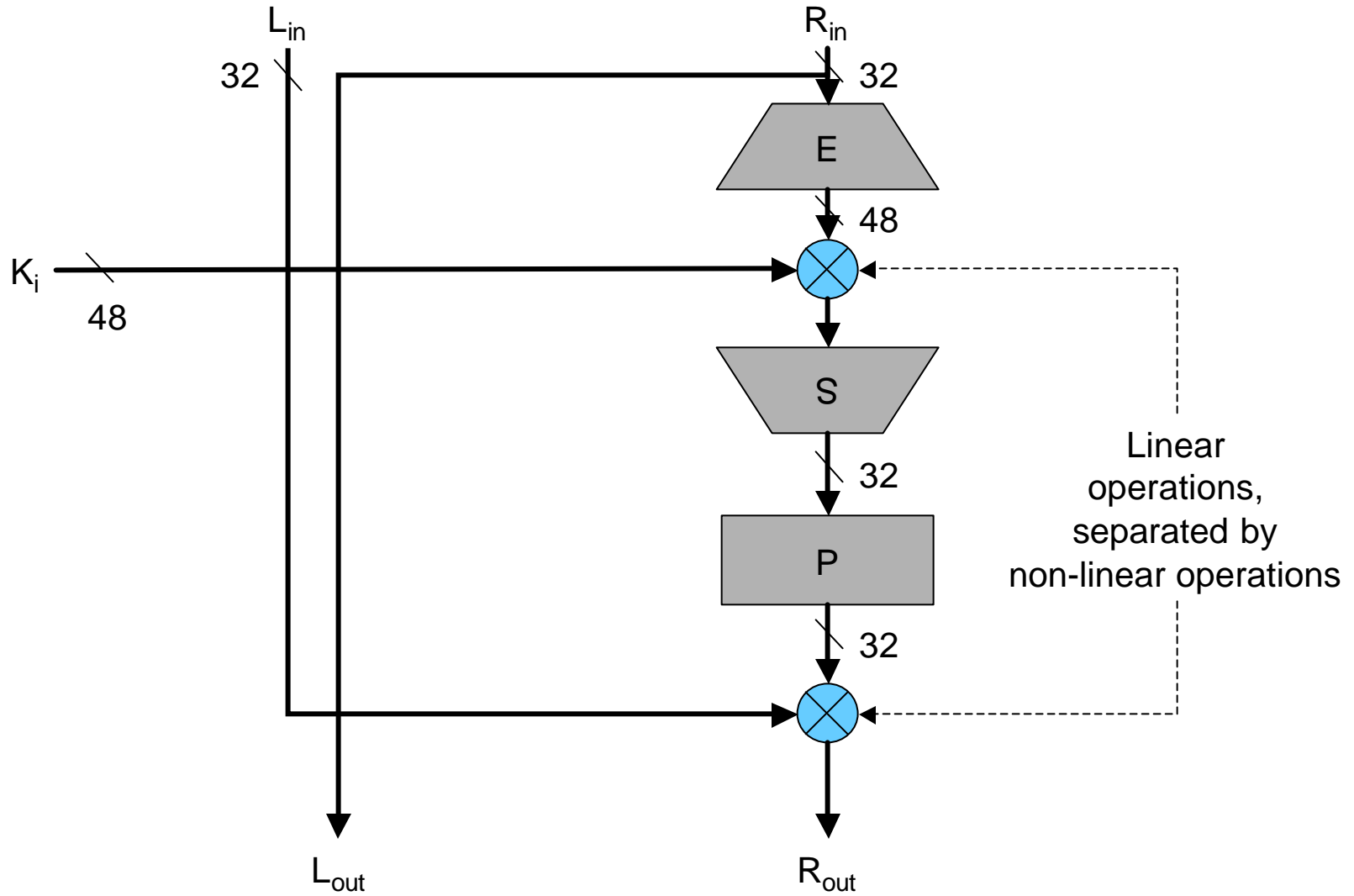
Internal operation of DES



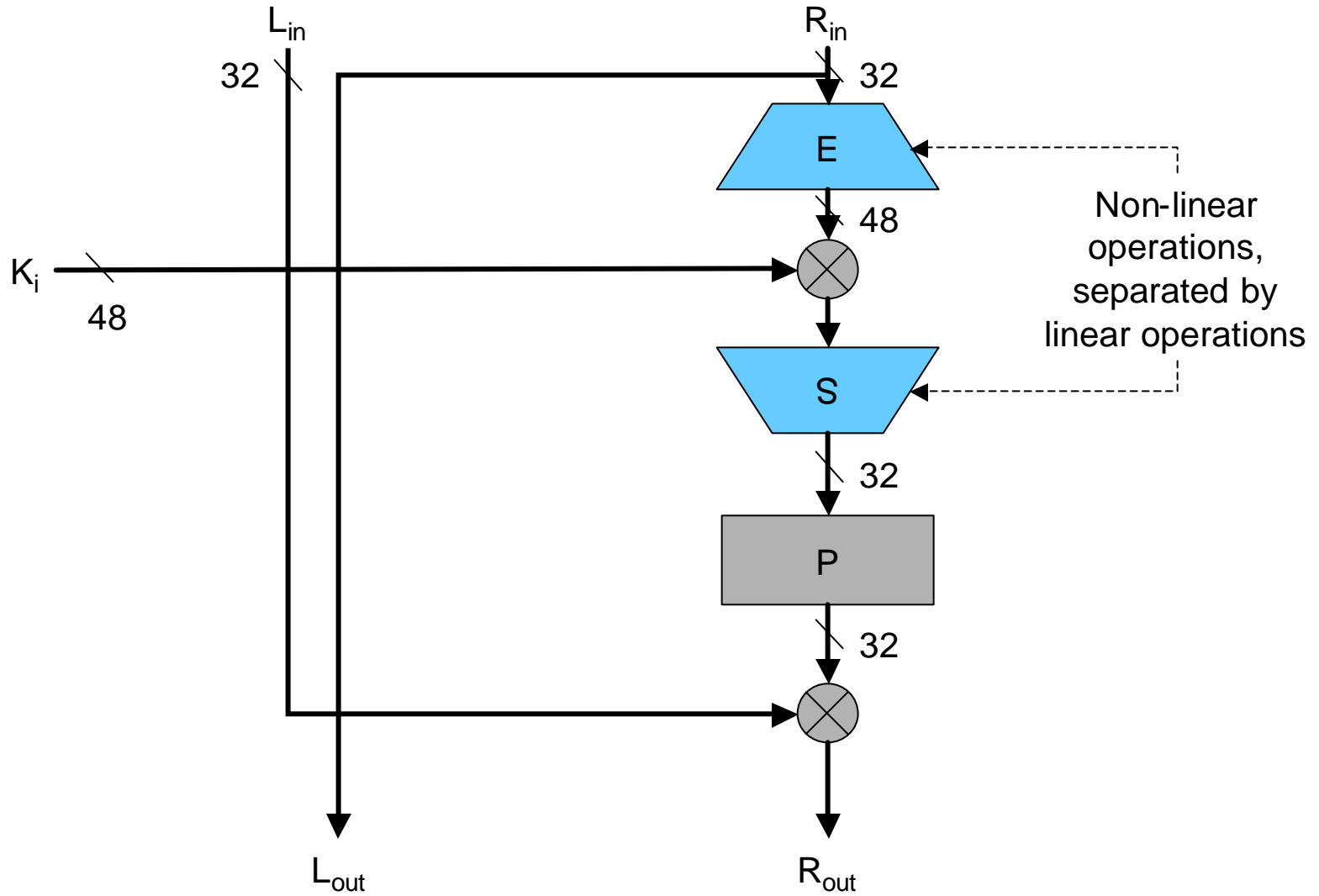
DES Round_i



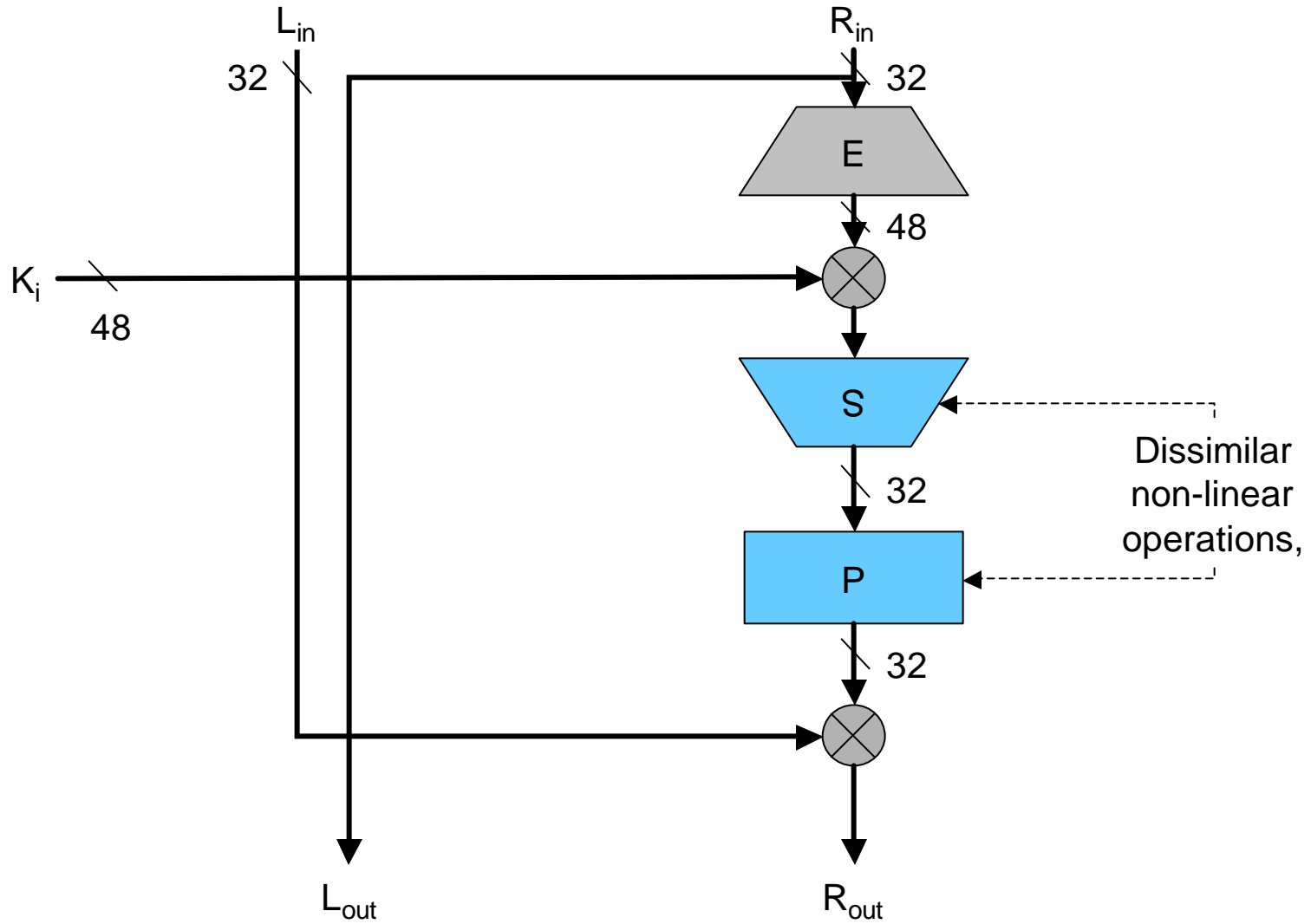
DES Round_i



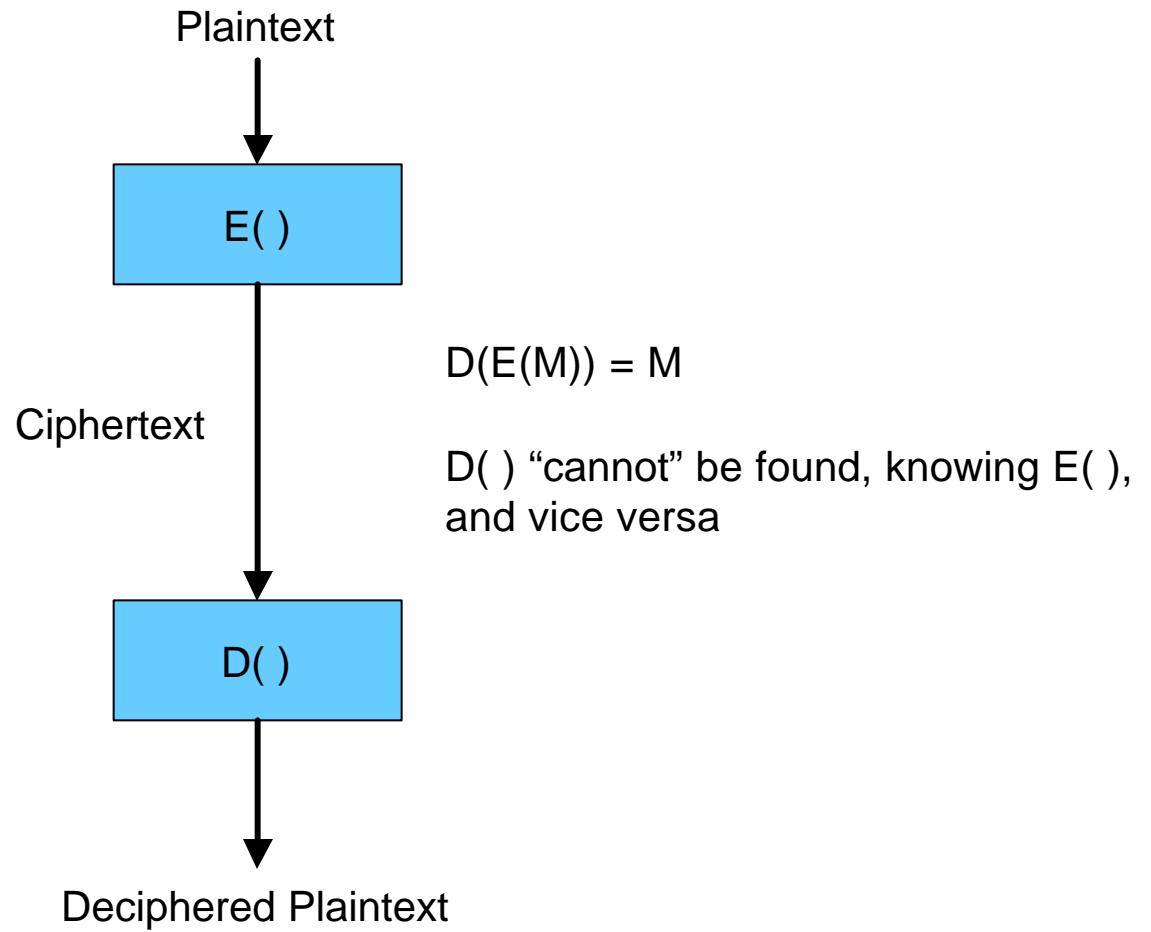
DES Round_i



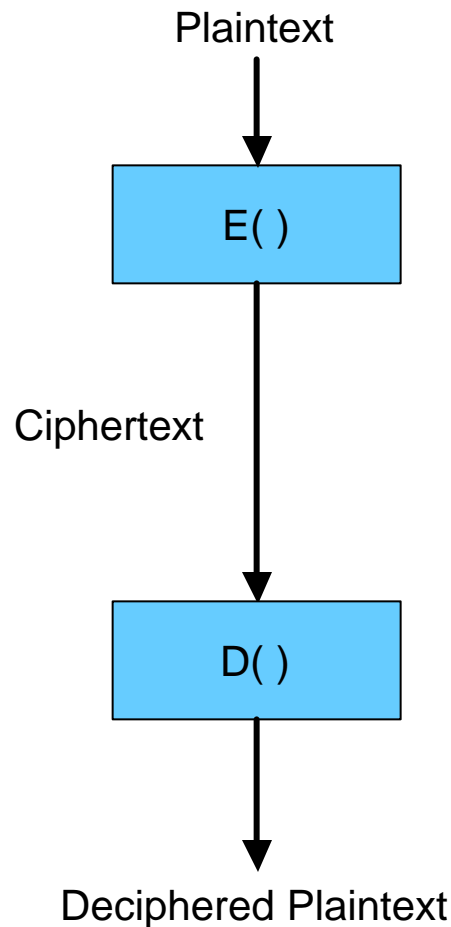
DES Round_i



Public Key Cryptosystems



Public Key Cryptosystems

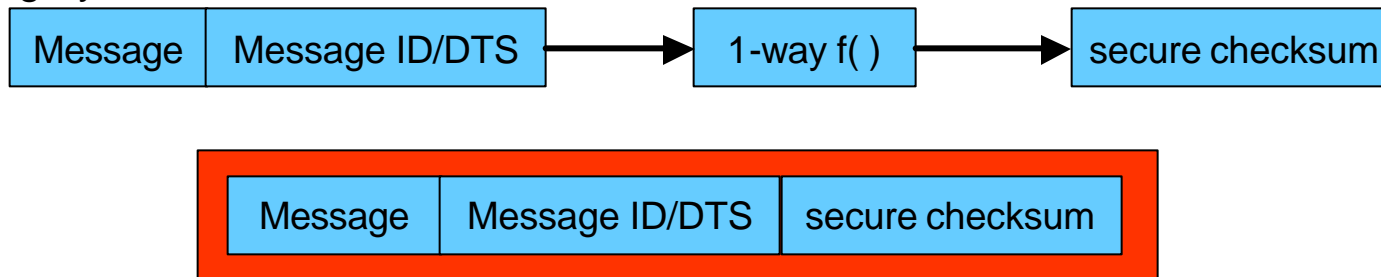


- $D()$ and $E()$ must be built on commutative functions:
 $f(g(x)) = g(f(x))$
- Multiplication and exponentiation work – are there others?
These form bases for Rivest-Shamir-Adleman (RSA) and Diffie-Hellman PKCs
- The apparent security of PKCs come from difficulty of computing logarithms and factoring composite numbers in a finite field. **Thought** to be NP-Complete problems, Which **might** make them mathematically intractable
- E.g.,
 $E(M) = M^e$
 $D(C) = C^d$
 $D(E(M)) = (M^e)^d = M^{ed} = M^1$, if $d=e^{-1}$ in the field

Applications of cryptography to security

- Confidentiality – the most obvious application

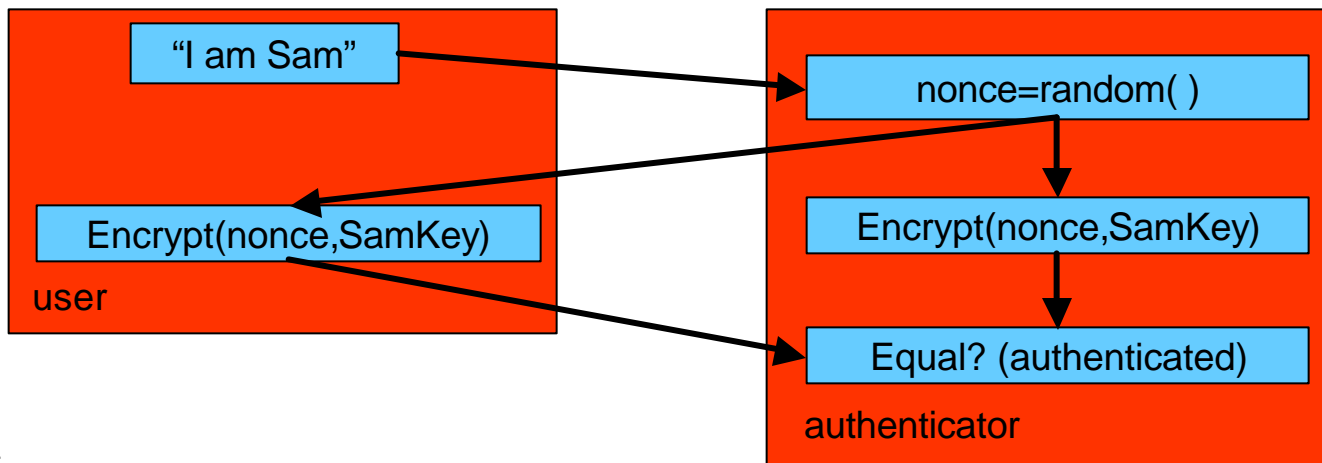
- Integrity



- Non-repudiation

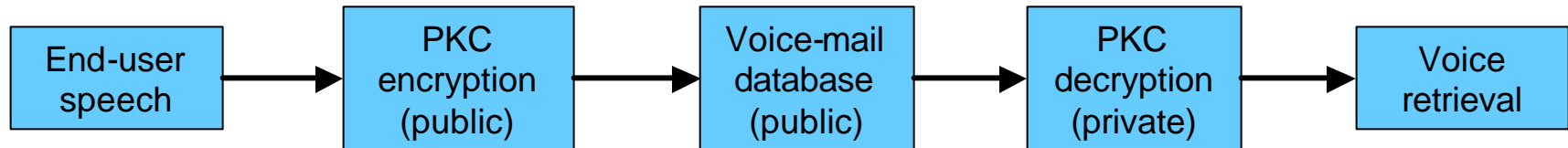
– Same as integrity, but seal the message: with user ID and user-specific key

- Authentication Challenge-response

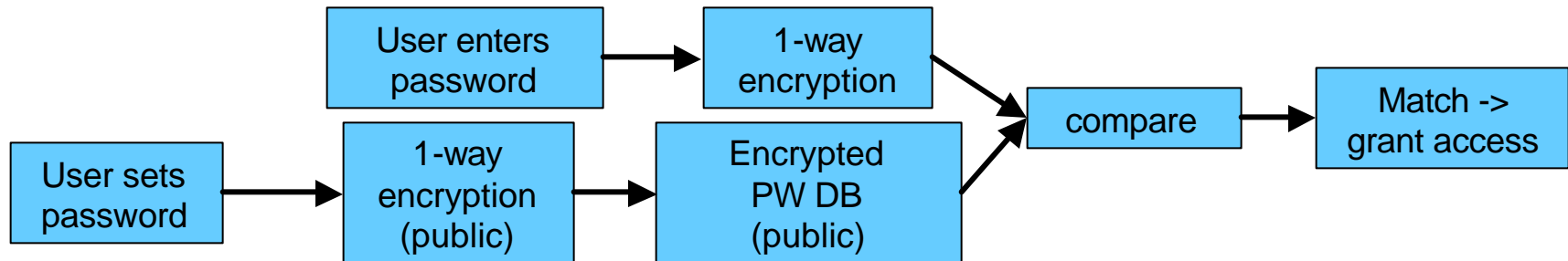


What can go wrong with cryptography?

- Gus Simmons' attack on voice mail system



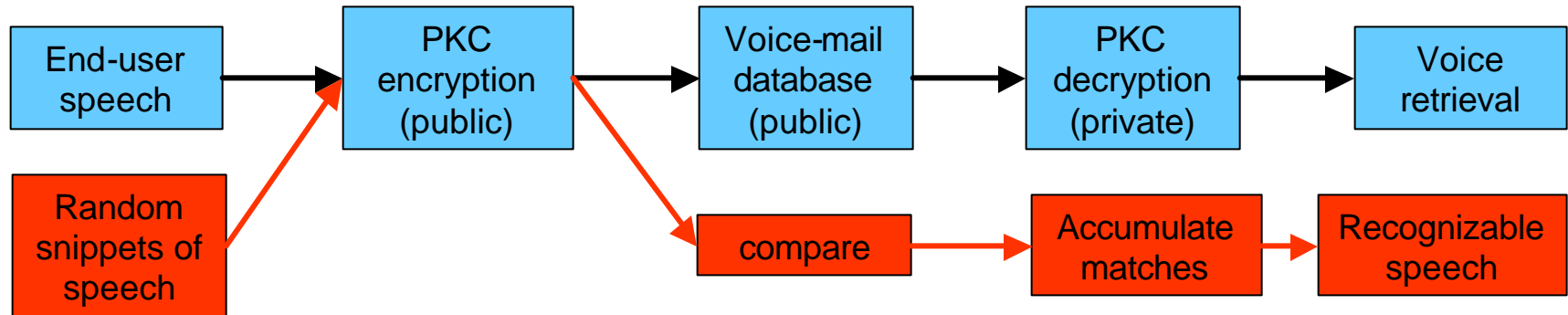
- Hacking UNIX passwords



- 802.11 WEP

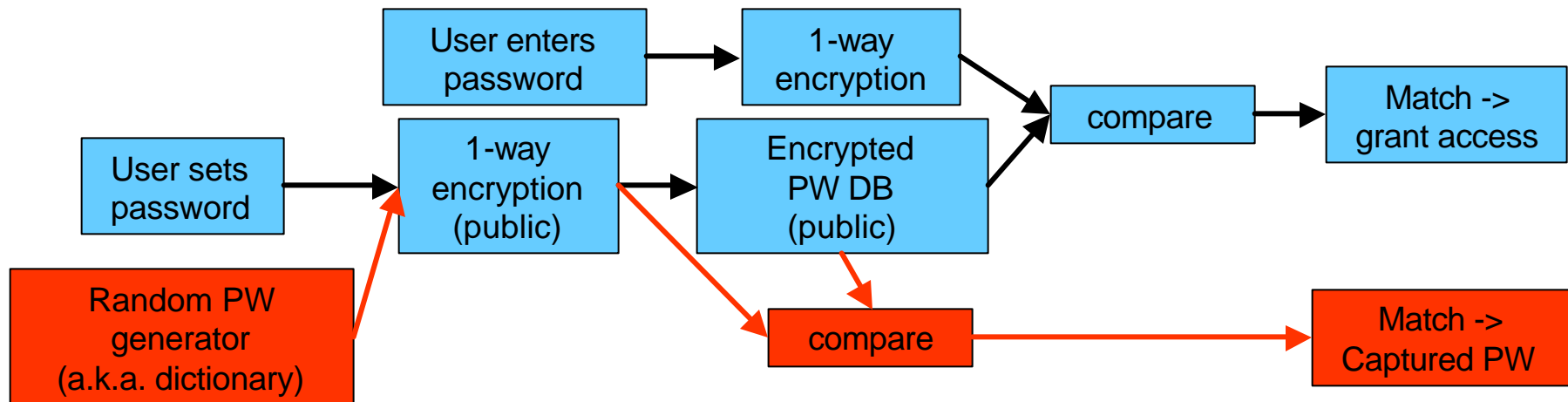
What can go wrong with cryptography?

- Gus Simmons' attack on voice mail system



Redundancy in Source Material

- Hacking UNIX passwords



- 802.11 WEP

Homework 2

“Wired Equivalent Privacy” (WEP) is the encryption protocol standardized in the IEEE 802.11 Wireless LAN standard. Hacker “warez” are readily available for download on the Internet to analyze WLAN traffic and recover the cleartext traffic.

Research the publicly available literature on WEP attacks and briefly summarize how these attacks work. Suggest a few simple changes that could be made to 802.11 that would have made these attacks much more difficult.